

Article

The Anticorruption Protocol to the United Nations Convention against Corruption Beneficial Owner Rule

Stuart S. Yeh

Department of Organizational Leadership, Policy, and Development, University of Minnesota,
Minneapolis, MN 55455, USA; yehxx008@umn.edu

Abstract: To fight corruption, money laundering, and organized crime, a proposed APUNCAC Beneficial Owner Rule would require financial service personnel to obtain and submit certification by the true beneficial owner when covered funds are transacted in amounts exceeding USD 3000. The strategy would trap front men into false statements, create a transaction-level record of assertions by front men that can be tested by a prosecutor, eliminate loopholes that allow criminals to escape prosecution in offshore havens, not require proof of a predicate crime or the illicit nature of funds, trigger a chain of witness cooperation, fight organized crime using a domino strategy, and be accomplished via a relatively simple change in domestic laws. Analysis suggests (1) the required technology exists; (2) transaction friction would be minimal; and (3) that the implementation of the Rule is feasible and practical, both operationally and from a legal standpoint, suggesting that the proposed Rule offers a promising strategy to fight organized crime.

Keywords: corruption; money laundering; organized crime; international law; international regulation; public policy; beneficial owner

Contents



Citation: Yeh, Stuart S.. 2023. The Anticorruption Protocol to the United Nations Convention against

Corruption Beneficial Owner Rule.

Laws 12: 86. <https://doi.org/10.3390/laws12060086>

Academic Editor: Patricia Easteal

Received: 8 July 2023

Revised: 23 September 2023

Accepted: 5 October 2023

Published: 24 October 2023



Copyright: © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction	3
2. The APUNCAC Beneficial Owner Rule	9
2.1. Financial Institutions	10
2.2. Banks	10
2.3. Individuals	10
2.4. Definitions	11
2.5. Addressing a Weakness	12
2.6. Summary	14
3. Issues	14
3.1. Definition of Beneficial Owner	15
3.2. A Flaw	16
3.3. Application of the Rule	17
3.3.1. Case 1: Corporation X Masquerading as a Restaurant	17
3.3.2. Case 2: Informal Peer-to-Peer Transfers	18
3.3.3. Case 3: Professional Service Intermediary	19
3.3.4. Case 4: Manipulation of Accounting Records	19
3.3.5. Case 5: Cuckoo Smurfing	20
3.3.6. Case 6: Invoice Manipulation	21
3.3.7. Case 7: Illicit Flows in Bolivia	22
3.4. Digital Identification	24
3.4.1. Norway	24
3.4.2. India	25

3.4.3. China	25
3.4.4. Japan	25
3.4.5. Indonesia	26
3.4.6. Russia	26
3.4.7. Argentina	26
3.4.8. Brazil	26
3.4.9. European Digital Identity	27
3.4.10. Africa	27
3.4.11. Global Adoption	29
3.4.12. MOSIP	29
3.4.13. ID2020	29
3.4.14. Digital ID Summary	30
3.5. Identity Proofing	30
3.5.1. What Is an ePassport?	32
3.5.2. How Is an ePassport Obtained?	32
3.5.3. How Many Countries Use ePassports?	32
3.5.4. Are ePassports from All Countries the Same?	32
3.5.5. Are ePassports More Secure than Traditional Passports?	33
3.5.6. What Security Measures Are Built into an ePassport?	33
3.5.7. Does Reading an ePassport Compromise the Security of the Information?	33
3.5.8. How Does a Border Official Determine That an ePassport Is Valid?	33
3.6. Dual Paired Certification	33
3.7. AML	34
3.8. TBML and IVTS	35
3.9. Front Men	38
3.10. Money Mules	39
3.11. Bank Clerks	40
3.12. Cooperation Agreements	40
3.12.1. Common Law Legal Systems	42
3.12.2. European Civil Law Systems	45
3.12.3. Non-European Civil Law Systems	47
3.12.4. Islamic Criminal Justice Systems	49
3.12.5. Cooperation Agreements—Summary	53
3.12.6. Viability of Cooperation Agreements	53
3.12.7. Implications	54
3.13. High-Volume Transactions	55
3.14. Rural Areas	56
3.15. No Electricity/No Internet	57
3.16. Transactions Involving Agents	57
3.17. Privacy Concerns	58
3.18. Exempt Transactions	58
3.19. Anonymous Instructions	58
3.20. Structuring	58
3.21. Beneficial Owner Is Not a Natural Person	58
3.22. Prohibition against Aiding and Abetting	59
3.23. Penalties	59
3.24. Enforcement	59
3.25. Extradition	62
3.25.1. Definitions	66
3.25.2. Extradition Thresholds	67
3.25.3. False Statements Risk Extradition	70
3.25.4. Extradite or Prosecute	71
3.25.5. Willingness to Prosecute	73
3.25.6. Serial Extradition	74

3.25.7. Reciprocity	76
3.25.8. A Genuine Threat	76
3.25.9. Aiding and Abetting	77
3.25.10. Conspiracy to Commit Money Laundering	79
3.25.11. Significance	82
3.26. INTERPOL Red Notice	83
3.27. Enforcement in Practice	83
3.28. Objective Territorial Principle	86
3.29. Effects Principle	87
3.29.1. United States	88
3.29.2. European Union	89
3.29.3. Significance	90
3.30. Extradition, Criminal Prosecution, and Cooperation—Antitrust Model	95
3.30.1. Acceptance of Effects Principle	95
3.30.2. Extradition of Foreign Nationals	99
3.30.3. Enablement of Cooperation Agreements	102
3.30.4. Summary	106
3.31. Extraterritorial Regulation—Examples	106
3.31.1. Title 18 Section 1956	107
3.31.2. FATCA	108
3.31.3. EMIR	109
3.31.4. MiFIR	110
3.31.5. Regulation 236/2012	110
3.31.6. Regulation 596/2014	111
3.31.7. Summary of Extraterritorial Regulations	111
3.32. International Agreements to Exchange Beneficial Ownership Information	112
3.32.1. IOSCO MMoU	112
3.32.2. EOIR/AEOI	113
3.32.3. CARF	115
3.32.4. 6AMLD	115
3.32.5. Regulation 2015/847	116
3.32.6. TFR	116
3.33. Implications	116
3.34. Benefits vs. Costs	117
3.35. Complicated Ownership Structures	119
3.36. Database Security	119
3.37. Political Concerns	120
3.38. Intercepted Communications	120
4. Discussion	122
5. References	128

1. Introduction

According to documents obtained by the International Consortium of Investigative Journalists (ICIJ), trillions in tainted dollars flow freely through major banks, exploiting loopholes in the international financial system, swamping a broken enforcement system, and facilitating human trafficking, sex trafficking, drug trafficking, terrorism, and transnational organized crime (ICIJ 2020). The enforcement system is overwhelmed, suggesting a need for aggressive changes.

According to a report by the Swiss Federal Office of Police, “the main obstacle to investigating money laundering is. . . lack of evidence. . . It is sometimes difficult to connect a suspicious financial transaction to a predicate offense, which is required [to prove] money laundering. . . In almost 2/3 of the cases of alleged money laundering of more than one million Swiss francs, the proceedings resulted in a dismissal” (FEDPOL 2014, p. 17). “The

main problem lies in criminal law. Prosecutors must... prove in each case that suspicious money comes from a crime... Without this evidence, Swiss prosecutors cannot prove money laundering” (Amicelle and Chaudieu 2022, p. 15).

There is a need for changes in criminal law so that prosecutors do not need to prove a link to a predicate offense. To address this issue, a proposed APUNCAC Beneficial Owner Rule would require financial service personnel to obtain and submit certification by the true beneficial owner when covered funds are deposited, transmitted, transferred, or paid in amounts exceeding USD 3000.¹ The APUNCAC Beneficial Owner Rule could not be avoided by criminals because the Rule would apply to all covered funds *whenever they are transmitted*. Suppose, for example, that a corrupt political figure sought to transmit funds offshore. The receiving jurisdiction might fail to require registration of beneficial ownership, but the state that is the source of the funds could choose to implement the APUNCAC Beneficial Owner Rule and apply the Rule to any person or entity that assists in transmitting funds offshore.

In an effort to subvert the Rule, a criminal may substitute a front man who would falsely certify that he is the true beneficial owner when, in fact, he is not (Figure 1).² However, a prosecutor who obtains communications directing the front man to send or receive funds could prove that the front man is not the true beneficial owner (because only the beneficial owner can issue instructions that control a financial transaction).³ It is not uncommon for prosecutors to obtain access to communications directing front men to send or receive funds (See Section 3.38). The availability of these messages, in combination with the Rule, would give prosecutors leverage over front men, enabling them to flip not only the front men but each person in the chain of command named by cooperating witnesses, leading to the top of the criminal organization, using a domino strategy.

Front men are weak links in criminal schemes. The APUNCAC strategy attacks this weak link. Front men can be pressured by prosecutors into cooperation agreements in exchange for a reduced or suspended sentence.⁴ A prosecutor would then utilize testimony from cooperating individuals to pressure implicated individuals into cooperation agreements. Each cooperating individual potentially provides information implicating higher-level individuals directing the lower-level criminals. In this way, a prosecutor could unravel even the most complex criminal scheme (see Section 3.3).

The proposed Rule targets low-hanging fruit, then uses a domino strategy to prosecute criminal leaders. The Rule would criminalize behavior that is currently not criminalized, permitting prosecutors to successively flip front men and every person in the organizational chain of command. Ultimately, testimony from key members of the organization would be used to prosecute the leaders.

The proposed change in law aims to open a flood of witness cooperation. Witness cooperation in the field of antitrust has been described as “the single most significant development in cartel enforcement” (Shaffer et al. 2015, pp. 337–38). When witnesses cooperate,

¹ Anticorruption Protocol to the United Nations Convention against Corruption, arts. 21(2)(a)(H), 21(3)(a)(viii), 21(3)(b)(viii), 22(1)(a)(G), 30(b), available at <https://tinyurl.com/y6bkpott>, accessed on 22 September 2023 [hereinafter APUNCAC]. The term “true beneficial owner” means the ultimate beneficial owner who controls the transaction for their benefit.

² “Front man” is a term of art that refers to an individual whose name is substituted for the name of the true beneficial owner in an effort to mislead authorities regarding the name of the true beneficial owner. I retain the term for clarity.

³ Text messages may include SMS text messages, email, or encoded Proton Mail or WhatsApp messages and may be obtained by prosecutors from electronic records, seized devices, or intercepted communications. See Section 3.38.

⁴ The APUNCAC strategy would require jurisdictions that currently do not utilize cooperation agreements to implement changes in law or practice that would permit such agreements. Each jurisdiction would make an independent judgment about the suitability of this strategy and would act accordingly. In the U.S., the U.S. Constitution protects the right of an accused person to remain silent, but this does not prevent prosecutors from obtaining independent evidence of culpability that may then be utilized to negotiate voluntary cooperation agreements in exchange for lesser charges. There is, in principle, no reason why voluntary cooperation agreements could not be utilized in other jurisdictions (See Section 3.12). The implementation of witness protection programs is discussed elsewhere (See Yeh 2022a, p. 40).

their testimony serves to crack criminal schemes, regardless of their sophistication. This permits prosecutors to reach the top of the organization. This approach has proven to be an efficient strategy to fight mafia figures and white-collar crime in the area of cartel enforcement and may be an efficient strategy to fight white-collar crime involving money laundering (See Section 3.30.3).

The Rule does not seek to identify the true beneficial owner by tracing genealogy. Instead, the Rule requires the true owner to certify ownership, applies penalties for false statements, and traps nominees who make false statements.

Significantly, the Rule obviates the need to prove knowledge of a predicate crime or the illicit nature of transacted funds. A prosecutor could unravel the scheme without a need to prove the illicit nature of the funds.⁵ The prosecutor's leverage would derive entirely from catching front men and criminals in an illegal scheme to hide the beneficial owner. Investigations would be efficient and precise because they would rely upon precise information provided by cooperating witnesses (see Sections 3.12 and 3.30.3). There would be little guesswork or arduous piecing together of scraps of information from obscure documentary sources (regarding inaccessibility of information, see [van der Does de Willebois et al. 2011](#)).

The Rule does not require a transferor, who may have no knowledge of the true beneficial owner, to certify the origin of the funds. The Rule distinguishes the true beneficial owner from a person who serves as a transferor but is not the beneficial owner (Figure 2). The Rule requires the true beneficial owner of the funds to certify beneficial ownership. When the funds are retransmitted, but beneficial ownership does not change, financial personnel would submit the original certification of beneficial ownership by the true owner, satisfying the Rule.

A transferor who is not the true beneficial owner has no responsibility for supplying a certification of beneficial ownership (and is not permitted to supply certification). That duty is the sole responsibility of the true beneficial owner. If the true owner is unwilling or unable to supply certification, the transaction would not be legal. If it proceeds or involves the creation of false certificates, the offense would be punishable by imprisonment.

The APUNCAC strategy offers significant advantages over conventional anticorruption and anti-money laundering strategies. Instead of placing a burden of due diligence on counterparties who are, in most cases, simply not in a position to determine whether the source of funds is licit or illicit, the APUNCAC Beneficial Owner Rule places the burden on the true beneficial owners and their front men to speak truthfully about what they know to be true. If they choose to make false statements, the Rule applies criminal penalties (see Section 3.23).

⁵ Al Capone, the famous gangster, was prosecuted for and convicted of tax evasion. Order, United States v. Capone, Nos. 22852, 23232 (N.D. Ill. 24 October 1931), <https://catalog.archives.gov/id/55311738> (accessed 21 October 2023); *aff'd*, 56 F.2d 927 (7th Cir. 1932); *appeal dismissed*, 93 F.2d 840 (7th Cir. 1937). While he had committed serious crimes, including murder, prosecutors chose to pursue charges that could be proven. The result was that Al Capone was imprisoned, sending the message that criminals cannot escape. By analogy, money laundering is a more serious crime than making a false statement regarding beneficial ownership. However, it may be easier to prove that a criminal has made a false statement. If the result is that the criminal is convicted and imprisoned, the deterrent effect is the same. It sends the message that criminals cannot escape.

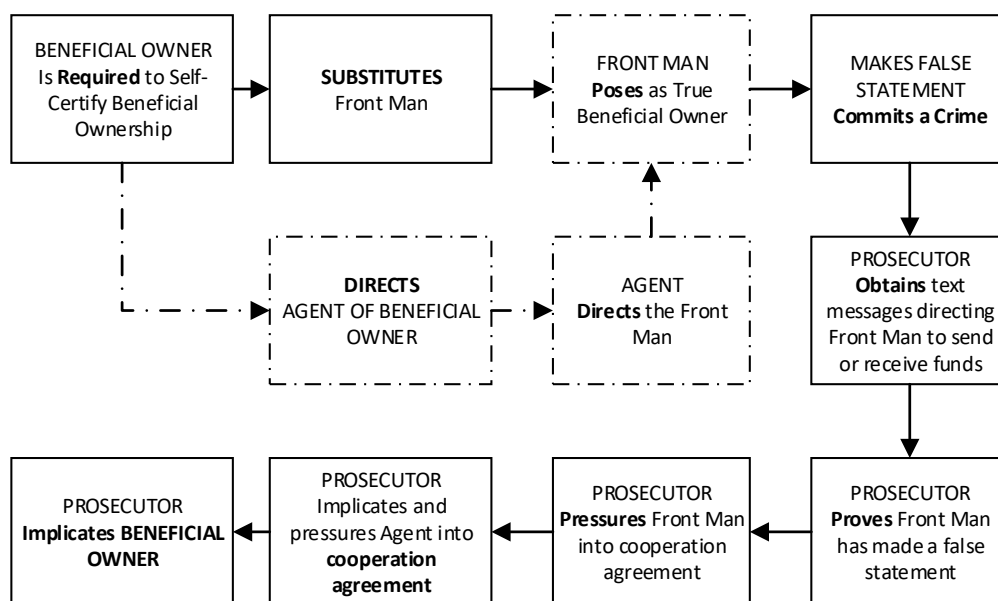


Figure 1. APUNCAC Beneficial Owner Rule traps front men into false statements.

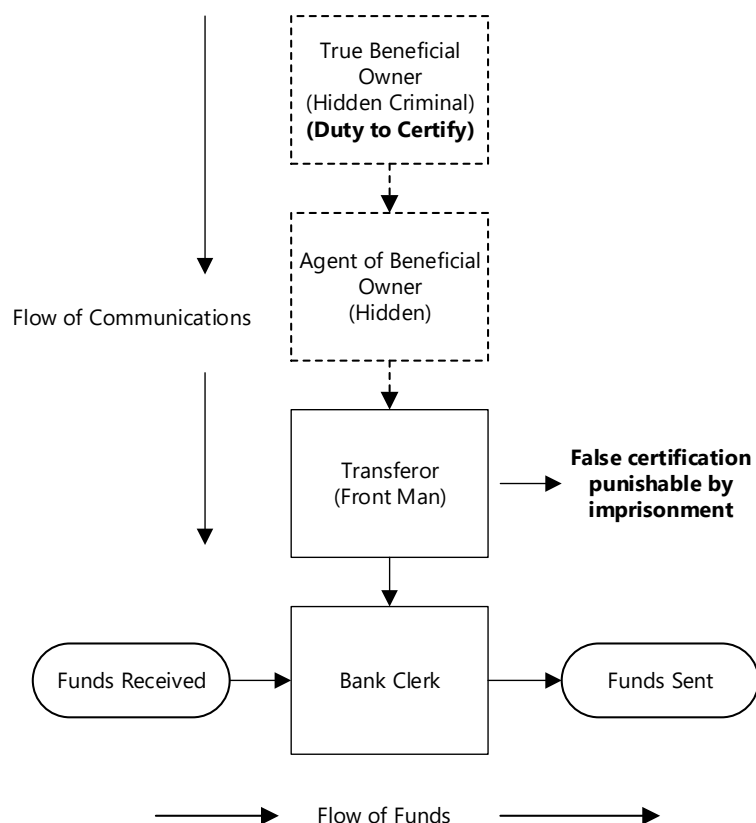


Figure 2. Hidden beneficial owner communicates via hidden agent with a transferor who serves as a front man posing as the true beneficial owner.

The APUNCAC strategy casts a wide net. It captures any scheme that involves front men. The strategy is suitable for addressing trade-based money laundering (TBML), *hawala* and other informal value transfer systems (IVTS), and money laundering involving crypto asset transfers, offshore havens, gaming, and casinos.⁶

There is a growing consensus regarding the need for the type of international beneficial owner reporting requirement that is at the heart of the APUNCAC strategy (see Sections 3.32 and 3.33). This article explains why a core group of nations concerned about money laundering and terrorist financing might be expected to adopt the APUNCAC Rule and write it into their criminal codes. This would satisfy the dual criminality requirement for extradition from one APUNCAC State Party to another (see Section 3.25). A violator of the Rule who visited an APUNCAC State Party would risk extradition and prosecution for violations of the Rule. Significantly, any financial service personnel who violated the Rule in any jurisdiction would risk prosecution if they were to travel to an APUNCAC State Party jurisdiction.

The effectiveness of this type of strategy is illustrated by the U.S. model of extraterritorial antitrust enforcement. The U.S. Department of Justice (DOJ) has been highly successful in obtaining extradition of foreign executives operating entirely outside the United States (Reims 2022, p. 8).⁷ The U.S. DOJ, via INTERPOL, obtains global Red Notices for wanted individuals. When violators of U.S. antitrust laws cross international borders, they are arrested and extradited to the U.S. for prosecution. The U.S. has prosecuted over 100 foreign nationals via this method (Reims 2022, p. 8).

The threat of extradition for violations of U.S. law is genuine. It imposes strong incentives to comply with U.S. law. Foreign executives who fall under U.S. law have voluntarily chosen to surrender, cooperate, and serve jail time because it may be expedient to cooperate in order to avoid harsh punishment in the event of extradition (Thomas and Stefano 2016, p. 5). Indicted foreign nationals who prefer to remain at large are essentially prisoners within their own country, fearing to travel internationally where they might be arrested and extradited to the U.S. (Thomas and Stefano 2016, p. 5). For these individuals, the threat of extradition poses “an imminent and ever-present peril, a modern sword of Damocles” (Thomas and Stefano 2016, p. 5).

In many cases, local law enforcement officials actively cooperate to arrest and extradite suspects, operating via mutual legal assistance treaties (MLATs). In other cases, individuals who actively enable money laundering because it is a profitable occupation may be susceptible to invitations to meet outside of their home jurisdictions. Authorities may find that suspects are willing to discuss and consummate plans to engage in illicit activities. After suspects are caught, prosecutors may negotiate cooperation agreements, permitting them to crack criminal schemes involving suspects engaged in criminal activities in offshore havens. The FBI, Europol, and U.S. Department of Justice (DOJ) have achieved success in pursuing suspects in notorious havens, including Panama, Malta, and Cyprus (Europol 2020; U.S. Mission Panama 2022; USDOJ 2020).

The Rule is intended for adoption by individual jurisdictions as domestic law, applied extraterritorially. Sections 3.28 and 3.29, below, describe the legal principles that provide the foundation for assertions of extraterritorial jurisdiction. Section 3.30 describes the antitrust model of extradition, criminal prosecution, and application of cooperation agreements to secure the cooperation of criminal defendants. Section 3.31 describes six examples of U.S. and EU laws and regulations that are applied extraterritorially. Section 3.32 describes six examples of international agreements to collect and exchange beneficial ownership information. Section 3.33 analyzes the implications of these examples for the proposed

⁶ *Hawala* is a popular informal system that accomplishes long-distance transfer of money without the movement of physical currency or telegraph or computer network wire transfers between banks. *Hawala* relies instead on the performance and honor of an enormous worldwide network of money brokers known as *hawaladars*. Most *hawaladars* are small businessmen who provide *hawala* services as a sideline operation.

⁷ *United States v. Piscioti*, SD Fla. (24 April 2014).

Rule. Section 3.34 infers, from these examples, an international consensus that the benefits of collecting and exchanging beneficial ownership information exceed the costs.

Sections 3.29–3.31 articulate the source of law for the APUNCAC Rule—a combination of the effects principle, plus court rulings applying the effects principle to cases involving domestic laws asserting extraterritorial jurisdiction, plus global international acceptance among major states, exemplified by compliance with extradition requests and requests that accused individuals surrender to the authorities of regulating states.

The Rule would involve an assertion of extraterritorial jurisdiction in the same way that the U.S. Sherman Act or U.S. money laundering statutes are applied extraterritorially.⁸ Extraterritorial enforcement would rely upon application of existing extradition treaties, including the extradition provisions of the United Nations Convention against Transnational Organized Crime (UNTOC).⁹ Section 3.25 describes multiple paths that a prosecutor may pursue to achieve extradition and prosecution.

The proposed APUNCAC strategy offers a potential solution to major barriers that stymie prosecution when criminals layer the funds in question via opaque corporate entities nested like Russian dolls and registered in financial havens such as BVI, Malta, Cyprus, or Panama. Attempts by investigators to penetrate these schemes may take years. By the time investigators identify the natural persons involved and their relationships, the criminals employing the entities have disappeared. In contrast, the Rule would force criminals to submit, at the point of each transaction, the name of a single natural person who asserts beneficial ownership. A prosecutor would have immediate access to that information via a centralized database. A prosecutor would have immediate access to transaction-level assertions regarding beneficial ownership that can be tested, i.e., by obtaining access to communications directing that person to send or receive funds, thereby proving the person is not the true beneficial owner, creating prosecutorial leverage to force a cooperation agreement, triggering a chain of witness cooperation, and unraveling the scheme.

The Rule would force declaration, for each transaction, of the true beneficial owner, creating a record of testable assertions that can be impeached by a prosecutor, typically by obtaining access to communications directing front men to send or receive funds. A prosecutor would have the ability to slam the door shut with an ironclad case against an offshore criminal. In contrast, prosecutors currently struggle to touch offshore criminals outside of a prosecutor's jurisdiction. The proposed strategy would equip prosecutors with a potent extraterritorial law, functioning as a travel rule, to reach criminals operating in offshore havens. This offers a major advantage in situations where crime persists because criminals operate beyond a prosecutor's reach.

In sum, there are nine advantages of the proposed strategy:

1. It traps front men.
2. It triggers a chain of witness cooperation.
3. It does not require proof of a predicate crime or the illicit nature of funds.
4. It captures offshore behavior by non-state party nationals via a travel rule.
5. It fights organized crime using a domino strategy.
6. It would be accomplished via a relatively simple change in domestic laws.
7. For each transaction, prosecutors would have immediate access to the name of a single natural person who asserts beneficial ownership.
8. Prosecutors would have immediate access to a transaction-level record of assertions by front men that can be tested by a prosecutor.
9. The strategy eliminates loopholes that allow criminals to escape prosecution in offshore havens.

⁸ Sherman Act (1890), 26 Stat. 209, 15 USC §§ 1–7; 18 USC § 1956.

⁹ United Nations Convention Against Transnational Organized Crime, *opened for signature* 12 December 2000, 2225 UNTS 277 [hereinafter UNTOC].

The purpose of this article is to address numerous practical, operational, and legal issues. Analysis suggests (1) the required technology exists; (2) transaction friction would be minimal; and (3) that the implementation of the Rule is feasible and practical, both operationally and from a legal standpoint. This suggests that the proposed Rule offers a promising strategy to fight organized crime.

2. The APUNCAC Beneficial Owner Rule

The Rule was originally drafted as an element of a model international convention, the Anticorruption Protocol to the United Nations Convention against Corruption (APUNCAC).¹⁰ APUNCAC Article 74 stipulates:

Each State Party shall give effect to this Protocol and shall adopt such measures as may be necessary: (a) to establish as criminal offenses under its domestic law the offenses established in accordance with this Protocol; (b) to establish its jurisdiction over such offenses, in its territories and outside its territories; and (c) to make those offenses punishable by a maximum term of imprisonment not less than five years.¹¹

However, nothing prevents the Rule from being adopted and implemented into domestic law unilaterally, with extraterritorial effect (see Section 3.29 and the precedents described in Sections 3.30 and 3.31).

Therefore, I propose that the Rule be adopted by the member states of the Financial Action Task Force (FATF). The FATF has promulgated 40+9 (49) anti-money laundering recommendations that are treated by member states as mandatory standards. The FATF holds countries to account if they do not comply with the standards by placing noncompliant countries on “grey” and “black” lists, involving onerous restrictions. FATF adoption of the proposed Rule would essentially involve the adoption and implementation of the Rule by FATF member states plus member states of FATF-style regional bodies. In total, 200+ jurisdictions have committed to the adoption of FATF recommendations, implying that the adoption of the Rule would potentially influence the legal and regulatory regime in 200+ jurisdictions (FATF 2019a, p. 72; 2021). Adoption by FATF would have far-reaching consequences throughout the international financial system.

The Rule is articulated in the form of three articles, focusing on non-bank financial institutions, banks, and individuals, respectively, to be adopted by potential States Parties. The Rule covers wire transfers, crypto transfers, peer-to-peer transfers, *hawala* transfers, and transactions involving monetary instruments, including currency, cryptocurrency, and bearer instruments. Payment via credit card, debit card, personal check (not in bearer form), mobile payment (not involving cryptocurrency), or automated clearing house (ACH) avoids application of the Rule. Electronic fund transfers (not involving cryptocurrency) initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account, including point-of-sale transfers, automated teller machine (ATM) transfers, direct deposits or withdrawals of funds, transfers initiated by telephone, transfers resulting from debit card transactions, whether or not initiated through an electronic terminal, and any other funds transfers that are made through an automated clearinghouse, an ATM, or a point-of-sale system are also excluded.¹² To the extent that those types of transactions are adequately regulated, investigators may follow the money trail. A jurisdiction may, as needed, remedy gaps in domestic law and regulation.

¹⁰ APUNCAC, available at <https://tinyurl.com/y6bkpott>, accessed on 22 September 2023.

¹¹ APUNCAC art. 74.

¹² To the extent that ATM daily cash withdrawal limits typically fall below the USD 3000 APUNCAC Rule threshold, the exemption for ATM withdrawals would not have a material effect.

2.1. Financial Institutions

APUNCAC Article 21 would regulate non-bank financial institutions. The relevant language states:

Each agent, agency, branch, or office of a financial institution other than a bank: (i) within the jurisdiction of a State Party, or (ii) that handles an international funds transfer in the amount of \$3000 or more—(A) on behalf of, or for the benefit of, a national of a State Party, or an entity within the jurisdiction of a State Party or (B) that is transmitted to or from the jurisdiction of a State Party; shall with respect to a transmittal of funds in the amount of \$3000 or more. . . retain and submit to FINCEN an electronic record of the following information relating to the transmittal order. . .

Certification of the source and beneficial owner of the source funds, and the beneficial owner of the receiving account (or, in the case of a trust, the potential or actual individually identified trust beneficiaries), certification that such funds do not involve the laundering of funds obtained illegally or through criminal activities and do not involve tax evasion, and acknowledgment that criminal penalties apply if false or misleading information is provided. . .

Alternatively, a beneficial owner of the source funds, or a beneficial owner of the receiving account, or his certified agent, may satisfy the applicable provisions of subparagraph (H) by (i) appearing in person at any time prior to such transmittal of funds pursuant to this paragraph, (ii) presenting his passport, and (iii) certifying beneficial ownership under penalty of perjury of all funds that are received by, or transmitted from, his account. Such one-time alternative certification shall be effective upon electronic submission to FINCEN in a form and manner determined by FINCEN.¹³

2.2. Banks

APUNCAC Article 22 articulates parallel requirements for banks.¹⁴

2.3. Individuals

APUNCAC Article 30 would regulate individuals. The relevant language states:

With the exception of individuals employed by banks that are exempted from currency transaction reporting requirements pursuant to Article 31, any person (hereinafter “covered person”) doing business, whether or not on a regular basis or as an organized business concern, who provides remittance services, makes or receives currency deposits or currency payments, or converts monetary instruments or virtual assets to currency as a financial service, and handles a transaction (deposit, withdrawal, exchange, or other payment or transfer) involving a monetary instrument or transmittal of funds with a value totaling \$3000 or more on a single day on behalf of a single person or entity, that is withdrawn, received, deposited, exchanged, paid, remitted, transmitted, or transferred by a national of a State Party, or is transmitted to, from, through, within, or with the assistance of a person or entity within the jurisdiction of, registered with, or within the territory of, a State Party, or any application or device performing the function of such covered person, shall. . .

Submit electronic certification to FINCEN of the source and beneficial owner of the source funds, and the beneficial owner of the receiving account (or, in the case of a trust, the potential or actual individually identified trust beneficiaries), certification that such funds do not involve the laundering of funds obtained

¹³ APUNCAC art. 21(2)(a)(H).

¹⁴ *Id.* art. 22(1)(a)(G).

illegally or through criminal activities and do not involve tax evasion, and acknowledgment that criminal penalties apply if false or misleading information is provided...

Alternatively, a beneficial owner of the source funds, or a beneficial owner of the receiving account, or his certified agent, may satisfy the applicable provisions of subparagraph (b) by (i) appearing in person at any time prior to such transmittal of funds pursuant to this paragraph, (ii) presenting his passport, and (iii) certifying beneficial ownership under penalty of perjury of all funds that are received by, or transmitted from, his account. Such one-time alternative certification shall be effective upon electronic submission to FINCEN in a form and manner determined by FINCEN.¹⁵

2.4. Definitions

APUNCAC defines “financial institution” to include a “money services business”, including a “currency dealer or exchanger”, defined as “a person who accepts currency, or other monetary instruments. . . in exchange for other forms of currency, or other monetary instruments”.¹⁶ The definition of a money services business (MSB) includes a “money transmitter”, defined as “a person who provides money transmission services”, involving the “acceptance of currency, monetary instruments, funds, or other value that substitutes for currency from one person and the transmission of currency, monetary instruments, funds, or other value that substitutes for currency to another location or person by any means”.¹⁷

“Currency” is defined to include fiat currency, virtual currency, or virtual assets.¹⁸ “Virtual currency” is defined as convertible virtual currency or legal tender digital currency.¹⁹ “Convertible virtual currency” (CVC) is defined as “a medium of exchange that has an equivalent value in fiat currency or acts as a substitute for fiat currency but is not legal tender digital currency”.²⁰ “Legal tender digital currency” (LTDC) is defined as “a digital form of fiat currency that is customarily accepted as a medium of exchange in the country of issue”.²¹ “Virtual asset” is defined as “a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes” including “virtual currency and online gaming keys, codes, and items of value that may be exchanged for fiat currency or legal tender digital currency”.²²

“Monetary instrument” is defined as:

(i) currency; (ii) travelers’ checks in any form; (iii) all negotiable instruments (including personal checks, business checks, official bank checks, cashier’s checks, third-party checks, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee (for the purposes of Article 20), or otherwise in such form that title thereto passes upon delivery; (iv) incomplete instruments (including personal checks, business checks, official bank checks, cashier’s checks, third-party checks, promissory notes, and money orders) signed but with the payee’s name omitted; (v) securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery; and (vi) value that substitutes for any monetary instrument described in subparagraph (i), (ii), (iii), (iv), or (v).²³

¹⁵ *Id.* art. 30.

¹⁶ *Id.* arts. 70(1)(kkk), 70(1)(iiii), 70(1)(qq).

¹⁷ *Id.* arts. 70(1)(iiii), 70(1)(llll), 70(1)(kkkk).

¹⁸ *Id.* art. 70(1)(pp).

¹⁹ *Id.* art. 70(1)(kkkkkk).

²⁰ *Id.* art. 70(1)(ll).

²¹ *Id.* art. 70(1)(dddd).

²² *Id.* art. 70(1)(jjjjjj).

²³ *Id.* art. 70(1)(ffff).

The Article 21 financial institution beneficial owner reporting requirement would regulate a “transmittal of funds” involving a “transmittal order” to transmit “money”.²⁴ The parallel Article 22 bank reporting requirement would regulate a “funds transfer” involving a “payment order” to pay “money”.²⁵ “Money” is defined as “a medium of exchange (i) currently authorized or adopted by a domestic or foreign government, (ii) virtual currency, or (iii) virtual assets”.²⁶

These definitions capture dealers, exchangers, and transmitters of cryptocurrency and digital assets that act as substitutes for fiat currency, as well as *hawaladars* (*hawala* brokers) and other individuals engaged in informal value transfers, in alignment with Financial Action Task Force (FATF) Recommendations (FATF 2019b, 2023).

The terms “transmittal of funds” and “funds transfer” include peer-to-peer transfers but exclude:

- (a) an electronic fund transfer initiated through an electronic terminal, telephone, computer, or magnetic tape, for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account, including point-of-sale transfers, automated teller machine transfers, direct deposits or withdrawals of funds, transfers initiated by telephone, transfers resulting from debit card transactions, whether or not initiated through an electronic terminal, and (b) any other funds transfers that are made through an automated clearinghouse, an automated teller machine, or a point-of-sale system.²⁷

These exclusions serve to exclude a range of fund transfers that are presumed to be adequately documented for investigative purposes, such as point-of-sale transfers, from the transmittals and transfers covered by Articles 21, 22, and 30.²⁸ The exclusions serve to delimit the scope of the Rule to focus on high-risk transmittals of funds that may be used for money laundering. Article 30 carves out (and covers) any transmittal or transfer involving a “monetary instrument”. The carveout from the exclusions ensures that high-risk transactions involving monetary instruments are covered by the Rule.

2.5. Addressing a Weakness

Article 30 regulates individuals who handle covered transactions, including retail transactions, involving the sale of goods or services, as well as the transmission of money. Article 30 regulates flows of money via the purchase and sale of goods and services, as well as the transmission of money from one person to another. Article 30 is designed to fill a gap in financial regulations that occurs when existing anti-money laundering regulations do not adequately regulate and do not require beneficial owner reports regarding cash or cash-like retail transactions and fail to address flows of money via the purchase and sale of goods and services.

Criminal penalties would be applied to individuals who do not comply with the requirements. The imposition of criminal penalties is a prerequisite to the implementation of leniency programs that permit accused individuals to exchange cooperation with authorities for a reduced or suspended sentence. This type of cooperation agreement is central to the APUNCAC strategy for fighting organized crime. Individual-level (versus institutional-level) accountability is intended to facilitate prosecution of recalcitrant individuals and promote compliance of front-line financial institution personnel.

Article 30 is similar in nature to the U.S. domestic requirement that any person who receives cash exceeding USD 10,000 while engaged in a trade or business must report the name, address, date of birth, taxpayer identification number, occupation, and identification document details of the individual from whom the cash was received, as well as the name,

²⁴ *Id.* art. 21(2).

²⁵ *Id.* art. 22(1).

²⁶ *Id.* art. 70(1)(hhhh).

²⁷ *Id.* arts. 70(1)(qqq), 70(1)(xxxxxx).

²⁸ A jurisdiction may, as needed, remedy gaps in domestic law and regulation.

address, taxpayer identification number, occupation, “alien identification” number and details of the person on whose behalf the transaction was conducted, plus the date of the transaction, the amount of cash received, the breakdown (U.S. currency, foreign currency, cashier’s checks, money orders, bank drafts, traveler’s checks), the type of transaction, a specific description of the property sold or service rendered, plus the name, address, and employer identification number or social security identification number of the business that received the cash (FinCEN 2014). The U.S. cash transaction report must be signed by an authorized individual who attests under penalty of perjury that the information is “true, correct, and complete” (FinCEN 2014).

A basic similarity is that both regulations seek to cover all types of retail transactions involving cash, require the collection and reporting of beneficial owner information, and require certification that the information is true, correct, and complete. While the U.S. requirement may seem onerous, it is a requirement that has proven to be operationally feasible, practical, and useful in the largest economy in the world. A difference, as explained in Section 3.4, is that the APUNCAC Rule could be implemented via digital technology in a way that would minimize transaction friction.

Articles 21 and 22 would regulate non-bank financial institutions and banks involved in the transmission (or payment) of money from one person to another. These regulations would ensure that the incentives for financial institutions are aligned with Article 30.

Article 21 would capture an administrator or exchanger that accepts and transmits cryptocurrency because the administrator or exchanger satisfies the definition of a money transmitter. The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies (including cryptocurrencies). Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter.

Article 30 would capture certain transactions that are not captured by Article 21 or 22 (Figure 3). For example, a user of cryptocurrency who obtains cryptocurrency and uses it to purchase real or virtual goods or services is not an MSB. Such activity, in and of itself, does not fit within the definition of “money transmission services” and is not covered by Article 21. However, the activity is covered by Article 30 because cryptocurrency is a monetary instrument.

If a broker or dealer in fiat currency or other commodities accepted and transmitted funds solely for the purpose of effecting a bona fide purchase or sale of the fiat currency or other commodities for or with a customer, such person would not be acting as a money transmitter and would not be covered by Article 21. However, that person would be captured by Article 30.

If the broker or dealer transferred funds between a customer and a third party that was not part of the currency or commodity transaction, such transmission of funds would no longer be a fundamental element of the actual transaction necessary to execute the contract for the purchase or sale of the currency or the other commodity. This scenario is, therefore, money transmission covered by Article 21, as well as Article 30. Examples include, in part, (1) the transfer of funds between a customer and a third party by permitting a third party to fund a customer’s account; (2) the transfer of value from a customer’s currency or commodity position to the account of another customer; or (3) the closing out of a customer’s currency or commodity position, with a transfer of proceeds to a third party.

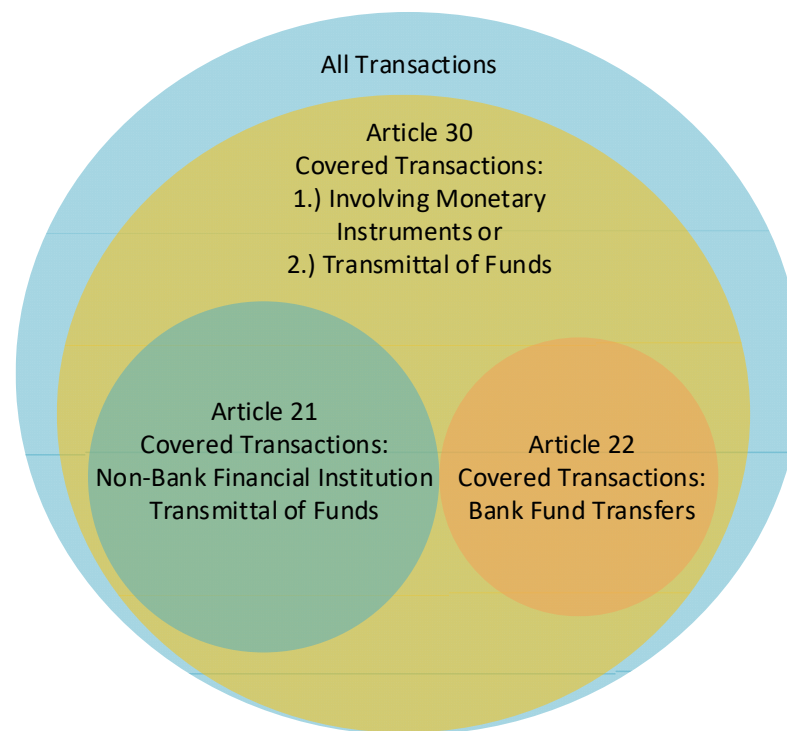


Figure 3. Article 30 captures certain transactions that are not captured by Article 21 or 22.

2.6. Summary

Table 1 summarizes the proposed application of the Rule. The Rule was specifically drafted to capture types of transactions that are especially vulnerable to money laundering, including international wire transfers, transactions in currency (including cryptocurrency), bearer instruments, certain negotiable instruments, certain bank drafts, and certain money orders. The Rule captures certain extraterritorial transactions if those transactions “touch” an APUNCAC State Party or its nationals, conducted outside the territory of APUNCAC States Parties (Table 1).

Table 1. Transactions (over USD 3000) covered by APUNCAC Beneficial Owner Rule.

Type of Transaction	Territorial Application	
	State Party ^a	Extraterritorial ^b
Wire transfer, crypto transfer, peer-to-peer transfer, or <i>hawala</i> transfer via <i>domestic</i> State Party bank or financial institution.	X	
Wire transfer, crypto transfer, peer-to-peer transfer, or <i>hawala</i> transfer via <i>extraterritorial</i> bank or financial institution (A) for national of (or entity in) State Party or (B) to or from State Party.		X
Transaction involving a monetary instrument or transmittal of funds (A) by national of State Party, or (B) transmitted to, from, or with assistance of person/entity within jurisdiction of State Party. ^c	X	X

Notes: ^a Domestic APUNCAC State Party territory. ^b Extraterritorial to APUNCAC States Parties. ^c Monetary instruments include fiat currency, cryptocurrency, and bearer instruments.

3. Issues

The issues raised by the proposed APUNCAC Beneficial Owner Rule include: the APUNCAC definition of “beneficial owner”; flaws in existing procedures for obtaining beneficial owner information; application of the Rule to money laundering schemes; availability and usage of the required digital identification technology; identity-proofing procedures; dual paired certification; the anti-money laundering (AML) effect of the Rule; application of the Rule to trade-based money laundering (TBML) and informal value transfer systems (IVTS);

how the Rule would genuinely threaten money laundering involving front men, money mules, and bank clerks; cooperation agreements; facilitation of high volume transactions; availability of the required technology in rural areas; procedures in the event of electricity or internet outages; transactions involving agents; privacy concerns; exempt transactions; anonymous instructions; structuring; transactions where the beneficial owner is not a natural person; aiding or abetting noncompliance with the Rule; penalties; enforcement of the Rule; extradition; extradition thresholds, including dual criminality; the responsibility to extradite or prosecute (*aut dedere aut judicare*); willingness to prosecute; serial extradition; reciprocity; application of the Rule to bank clerks and front men; definition of aiding and abetting serious crime; conspiracy to commit money laundering; use of INTERPOL Red Notices; enforcement in practice; the objective territorial principle; the effects principle; the antitrust model of extraterritorial enforcement; extraterritorial regulation; precedents for the international collection and exchange of beneficial owner information; benefits vs. costs; complicated ownership structures; database security; political concerns; and intercepted communications. Issues regarding extraterritorial jurisdiction, enforcement, and application of the proposed Rule to six case examples involving Danske Bank Estonia, the Vancouver Model, Liberty Reserve, the *hawala* system, online gaming, and cryptocurrency were addressed in prior publications (Yeh 2020a, 2020b, 2020c, 2021, 2022b).

3.1. Definition of Beneficial Owner

APUNCAC defines the beneficial owner as follows:

“Beneficial owner” (or “beneficiary”) of funds shall mean the natural person or persons who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise (i) exercises substantial control or (ii) owns or controls not less than 25 percent of the ownership interests of the funds. In the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

- (i) where the future beneficiaries have already been determined, the natural person(s) who is(are) the beneficiary of 25 percent or more of the property of a legal arrangement or entity;
- (ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
- (iii) the natural person(s) who exercise(s) control over 25 percent or more of the property of a legal arrangement or entity.

In the case of a legal entity customer where no natural person(s) directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise (i) exercises substantial control or (ii) owns or controls not less than 25 percent of the ownership interests of the funds, the beneficial owner is the legal entity.²⁹

In comparison, the U.S. Treasury Department, via FinCEN, requires the following individuals to complete a certification of beneficial ownership when opening an account:

- (i) Each individual, if any, who owns, directly or indirectly, 25 percent or more of the equity interests of the legal entity customer (e.g., each natural person that owns 25 percent or more of the shares of a corporation); and
- (ii) An individual with significant responsibility for managing the legal entity customer (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer). (FinCEN 2016).

²⁹ *Id.* art. 70(1)(p).

The APUNCAC definition of beneficial ownership omits the language regarding “an individual with significant responsibility for managing the legal entity customer”. This definition excludes senior officers from the requirement to self-certify beneficial ownership under the APUNCAC Beneficial Owner Rule unless they are controlling individual company-related transactions for their own direct benefit or unless they meet the 25 percent ownership threshold. If the FinCEN definition were to be applied, then the CEO of each company would always be listed as a “beneficial owner” for any transaction exceeding USD 3000. The APUNCAC definition serves to focus attention on transactions deserving investigative and prosecutorial attention.

In contrast, the APUNCAC definition would apply, for example, if a senior company officer chose to direct a payment exceeding USD 3000 out of company funds to a foreign official for the purpose of facilitating a contract negotiated by that officer. In that case, the foreign official personally benefits from the transaction and meets the 25 percent APUNCAC threshold (because the entire amount is for the benefit of the foreign official). The purpose of the payment is to facilitate a transaction that would not otherwise occur except for the intervention of the senior officer. This is the type of transaction that would justify investigative and prosecutorial attention and is the target of the APUNCAC Rule.

Operationally, FINCEN (the global version of FinCEN established by APUNCAC) could establish a rule that transmissions between two corporate accounts are not covered by the APUNCAC Beneficial Owner Rule except if either account is controlled by one, two, three, or four individuals for their own benefit.

While criminals may invent complicated ownership schemes designed to hide beneficial ownership, the definition of a true beneficial owner cuts through the form of ownership. If a natural person exerts control over a transaction for his/her own benefit, that person is a beneficial owner. It does not matter whether control is silent, involving an implicit agreement to serve the interests of a silent beneficial owner.

3.2. A Flaw

Existing procedures for obtaining beneficial owner information are flawed. In the U.S., the existing procedure for certifying beneficial ownership is illustrated by the procedure utilized by Wells Fargo Bank ([Wells Fargo 2021](#)). The Wells Fargo beneficial owner certification form describes the individual who must complete the form as “the person opening a new account”:

This form must be completed by the person opening a new account or maintaining business relationships on behalf of a legal entity with any of the following U.S. financial institutions: (i) a bank or credit union; (ii) a broker or dealer in securities; (iii) a mutual fund; (iv) a futures commission merchant; or (v) an introducing broker in commodities. For the purposes of this form, a legal entity includes a corporation, limited liability company, partnership, and any other similar business entity formed in the United States or a foreign country.

The form states the information to be provided:

This form requires you to provide the name, address, date of birth and social security number (or passport number or other similar information, in the case of non-U.S. persons) for the following beneficial owners:

- (i) Each individual, if any, who owns, directly or indirectly, 25 percent or more of the equity interests of the legal entity customer (e.g., each natural person that owns 25 percent or more of the shares of a corporation); and
- (ii) An individual with significant responsibility for managing the legal entity customer (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President or Treasurer).

The form states that presentation of a photo ID may be required:

The financial institution may also ask to see a copy of a driver's license or other identifying document for each beneficial owner listed on this form.

The form states, "I, [name of person opening the account], hereby certify, to the best of my knowledge, that the information provided above is complete and correct". The form provides a space for the named person to sign and date.

Thus, the person who opens the account provides the beneficial owner information and certifies that the information is complete and correct "to the best of" his or her knowledge. However, the person who opens the account may be an agent who has been informed that the beneficial owner is "X" when, in fact, the beneficial owner is "Y". Individual "X" may simply be a trusted front man who agrees to pose as the beneficial owner but is not in fact the true beneficial owner. If authorities later determine that the beneficial owner was not "X", the agent who opened the account may fall back on the assertion that the information provided was complete and correct "to the best of" his knowledge. A prosecutor would have difficulty proving otherwise, implying that neither the agent nor front men are likely to be deterred by the threat of prosecution.

This implies that existing procedures for obtaining beneficial owner information are flawed. If criminals can escape simply by asserting that the information was complete and correct "to the best of" their knowledge, the threat of prosecution is largely empty.

3.3. Application of the Rule

Six case examples illustrate the application of the APUNCAC Beneficial Owner Rule to: (a) 'Corporation X,' a seemingly legitimate firm that is used as a vehicle by 'F,' a criminal, to launder illicit funds, (b) 'April,' an innocent person who utilizes an informal value-transfer system to transfer licit funds, (c) 'Edgar,' a corporate services specialist who oversees a pooled bank account and a set of books to launder illicit funds, (d) a car dealer who utilizes a double set of books to launder illicit funds, (e) a 'cuckoo smurfing' scheme to launder illicit funds, and (f) an over-invoicing scheme to launder illicit funds.

3.3.1. Case 1: Corporation X Masquerading as a Restaurant

Suppose Corporation X, with equal shareholders A, B, C, D and E, is thinly capitalized. It has 1000 shares of USD 1 each, issued to the shareholders who are also the five directors of the company. It was set up to buy and operate a restaurant. It obtains a loan from F for USD 1 million. F happens to own the premises that the restaurant will lease. As Corporation X is thinly capitalized, the loan conditions are strict and allow a representative of F to attend and observe and speak, but not vote, at board meetings and allow F to immediately call (withdraw) the loan at any time that F may deem the investment to face undue risk. A question arises as to the persons who control the company and are the beneficial owner(s) in this scenario.³⁰

Regarding the APUNCAC Beneficial Owner Rule, none of the five shareholders and directors (individuals A, B, C, D, or E) meet the 25 percent threshold. They would not be required to observe the APUNCAC Beneficial Owner Rule, except for a transaction where the purpose is for the personal benefit of the sender or receiver, for example, involving a facilitation payment by "A" to a person "Z" (or vice-versa) regarding a contract negotiation. In that circumstance, the recipient of the facilitation payment personally benefits from the transaction. The payment is intended for the personal use of the recipient. The recipient is 100 percent beneficiary of the transaction and, therefore, subject to the Rule. The Rule targets transactions where either the sender or the recipient personally benefits from the transactions.

A second issue arises if the creditor exerts more influence and control than any of the shareholders and directors. If the creditor exerts this influence in a way that benefits all shareholders equally, i.e., by maximizing profits rather than disproportionately benefiting the creditor—the creditor would not qualify as the beneficial owner controlling the

³⁰ Scenario posed by Louis de Koker (personal communication, 15 September 2022).

transactions for his personal benefit and would not be subject to the Rule. In this scenario, however, “F” could be a criminal who inserts a cooperative associate (“K”) as head of procurement and ensures that the business appoints F’s contacts as service providers to the business. Through this scheme, F launders dirty money through the company accounts via seemingly legitimate corporate transactions. Recipients would be business creditors and would not stand out as unusual.

In this scenario, “F” is the criminal mastermind who directs “K”, the head of procurement. Presumably, “F” transmits messages (perhaps text messages), directing “K”, who then directs his subordinates regarding the financial transactions that involve money laundering. In this case, the beneficial owner is “F” because he is controlling the transactions for his personal benefit. Because the transactions meet the APUNCAC 25 percent threshold, they are subject to the Rule.

In this scenario, the subordinates of “K” are the individuals who implement the transactions. Under the APUNCAC Rule, a director (either A, B, C, D, or E) would be required to certify that there is no natural person who meets the APUNCAC definition of beneficial owner—i.e., that the beneficial owner, for the purpose of the APUNCAC transaction reporting rule, is Corporation X.³¹

In this scenario, a prosecutor suspects that F is laundering money via a legitimate business. The prosecutor obtains a warrant that permits the prosecutor to seize electronic devices. The prosecutor accesses text messages from “K” to his subordinates, directing them to implement the transactions—prima facie evidence that “K” is controlling the transactions and is (at least potentially) the “beneficial owner” controlling the transactions. If “K” personally benefits from the transactions and cannot identify a person who directed “K” to implement the transactions, then “K” is the person who controls the transactions and is, by definition, the beneficial owner. “K” would, to avoid criminal penalties imposed by APUNCAC for violations of the Rule, presumably choose to cooperate and name “F” as the person who directed “K”.

This pressure from the prosecutor to name “F” as the person directing the transactions would only exist if the Rule was implemented. The Rule criminalizes the act of not reporting a transaction when that transaction is for the personal benefit of an individual. Directors A, B, C, D, and E may or may not be aware of the criminal scheme. However, the prosecutor would be able to pressure K into a cooperation agreement where K would explain the scheme.

3.3.2. Case 2: Informal Peer-to-Peer Transfers

Trade-based money laundering and informal value transfer systems are used by criminals to obscure the source of illicit funds. However, the same value transfer systems are used by legitimate persons for legitimate reasons. Suppose, for example, that April, one of my daughter’s friends, needs to send money to my daughter to purchase concert tickets. April hands me USD 3000 in currency, then asks me to transmit USD 3000 to my daughter. The explanation could be perfectly innocent: April wishes to utilize my capacity to transmit the USD 3000 electronically, via my smartphone, to my daughter, who also has a smartphone. However, if April happened to be a criminal, she might utilize this path to hide the origin of the funds.

The APUNCAC Beneficial Owner Rule would not apply unless I operated a money services business (MSB). If, however, I operate an MSB, the Rule would apply, and I would be obligated to obtain a digital certification of beneficial ownership from April (the sender), plus a digital certification of beneficial ownership from my daughter (the recipient). This could be accomplished by initiating the transaction via my smartphone. A dedicated app on my phone would require April to confirm her identity (ideally, via biometric identification), then require her to confirm that she certifies beneficial ownership of the funds (as sender). My daughter would be required to complete a parallel procedure.

³¹ APUNCAC arts. 21(2)(a)(H)(2), 21(3)(a)(viii)(B), 21(3)(b)(viii)(B), 22(1)(a)(G)(2), 30(b)(2).

She would confirm her identity (ideally, via biometric identification), then confirm that she certifies beneficial ownership of the received funds. I would digitally certify my identity and electronically submit, via the dedicated app, the set of digital certifications to a global version of FINCEN. The transaction would then meet the requirements of the APUNCAC Beneficial Owner Rule.

To reiterate, the Rule requires the true beneficial owner to certify beneficial ownership. In this example, April is the true beneficial sender, not me, because she controls the transmission of the funds. The funds would not be sent in the absence of April's instruction to send the funds.

In this example, the Rule would apply if I was an MSB because the transaction involves currency and because it involves a transmittal of funds from me to my daughter via a peer-to-peer payment app.

3.3.3. Case 3: Professional Service Intermediary

Suppose that Edgar, a seemingly legitimate corporate services specialist, oversees a pooled bank account and a set of books that he uses to launder money for criminals (Murray 2016, pp. 450–51). He arranges for dirty cash pick-ups from Hector, a nightclub owner whose premises act as a drop venue for criminal funds. The cash that is collected by Edgar is used to settle debts owed to other subscribers to Edgar's services. Certain "subscribers" are, in fact, criminals. The fiction of "debt settlement" hides the illicit origin of the funds and serves to convert dirty money into seemingly clean money. The dirty cash pick-ups are not recorded in the official corporate service accounting records. Instead, the relevant accounting information that records the relevant debts and their settlement is maintained via secret records that are encrypted, hidden, or exist only in Edgar's head. There is no transmission through any bank account or financial institution, and, therefore, none of this activity would be included in a bank's Suspicious Activity Report (SAR). The essence of Edgar's scheme is that there is no provable link between the funds and any predicate crime. Therefore, it is extremely difficult to prove money laundering.

Conventional AML regulations fail to address this type of activity (Murray 2016, pp. 450–51). In contrast, the APUNCAC Beneficial Owner Rule would require Edgar and Hector to obtain certification of beneficial ownership from the true beneficial owners for each cash transaction exceeding USD 3000. If Edgar and Hector are front men for criminals who orchestrate the transactions, and if they falsely certify beneficial ownership as receiver and sender of the funds, they become vulnerable to prosecution if a prosecutor manages to obtain access to text messages from a third party (e.g., from seized mobile phones) directing them to send or receive the funds. If a third party is controlling the transactions, then Edgar cannot be the true beneficial recipient, and Hector cannot be the true beneficial sender of the funds. Having been caught making false statements and vulnerable to prosecution for making false statements, Edgar and Hector have a choice. They may either cooperate with the prosecutor and identify the third party, or they may risk imprisonment. If they cooperate and identify the third party, the criminal scheme is unraveled, and the prosecutor can go after the criminal orchestrating the transactions.

3.3.4. Case 4: Manipulation of Accounting Records

Suppose that criminals pay cash to a car dealer, but the payments are kept off the car dealer's official accounting books and, instead, are recorded in a set of secret accounting records hidden from authorities (Murray 2016, pp. 453–54). The car dealer uses the funds to purchase cars. The cars are sold to legitimate customers, who pay via cheque, credit card, or loans. The vehicle sales are recorded in the dealer's official accounting books and business records. The car dealer records fake payments to fictitious vehicle sellers in the dealer's official accounting books and business records. To settle debts with the criminals, the dealer diverts money out of company funds to a private account in the name of the proprietor's girlfriend.

Through this scheme, the flow of illicit funds is disguised by records of legitimate purchases by legitimate customers. The legitimate purchases create a paper trail via the dealer's books and business records that can be used to deflect the attention of suspicious authorities since apparently legitimate customers buy and pay for cars, creating legitimate flows of funds into and out of the car dealer's accounts. This circuitous scheme serves to launder the illicit funds. However, there is no evidence of a predicate offense, making it extremely difficult to prove money laundering.

Conventional AML regulations fail to address this type of activity (Murray 2016, pp. 453–54). In contrast, the APUNCAC Beneficial Owner Rule would require the car dealer to obtain certification of beneficial ownership, from the true beneficial owners, for each cash transaction exceeding USD 3000. The Rule prohibits any person or entity from acting in a manner that seeks to evade or assists in evading the Rule. If the car dealer serves as a front man and falsely certifies beneficial ownership of the funds, he becomes vulnerable to prosecution if a prosecutor manages to obtain access to text messages (e.g., from a seized mobile phone) directing the car dealer to send or receive funds. If someone other than the car dealer is controlling the transactions, then the car dealer cannot be the true beneficial owner of the funds. Having been caught making a false statement, and vulnerable to prosecution for making a false statement, the car dealer has a choice. He may either cooperate with the prosecutor and identify the criminal controlling the transactions or risk imprisonment. If he cooperates and identifies the criminal, the scheme is unraveled, and the prosecutor can go after the criminal orchestrating the transactions.

3.3.5. Case 5: Cuckoo Smurfing

Cuckoo smurfing is a form of money laundering where illicit funds are intermingled with legitimate fund transfers to hide their illicit origin. In this scheme, legitimate fund transfers are channeled via a central controller (Figure 4). Illicit fund transfers are channeled via the same controller. However, the legitimate funds are diverted to criminal beneficiaries, while the illicit funds are diverted to legitimate transferees. In this way, it appears that the criminals are receiving clean funds from legitimate transferors.

The example depicted in Figure 4 involves innocent UK individuals who are expecting deposits to be made into their accounts from innocent relatives in Pakistan. The legitimate transfers from these relatives, however, have been diverted by the transferring agent in Pakistan to a cash pool from which transfers are made to criminal beneficiaries. Illicit cash is simultaneously pooled, then transmitted to innocent individuals in the UK. In this way, it appears that the criminal beneficiaries are receiving clean funds from legitimate transferors.

Conventional AML regulations fail to address this type of activity (Murray 2016, pp. 454–55).³² In contrast, the APUNCAC Beneficial Owner Rule would require the bank clerks handling the cash deposits to obtain certification of beneficial ownership from the true beneficial owners for each cash transaction exceeding USD 3000. The Rule would also require the transfer agent in Pakistan to obtain certification of beneficial ownership from the true beneficial owners for each wire transfer exceeding USD 3000. If front men falsely certify beneficial ownership of the funds, they become vulnerable to prosecution if a prosecutor manages to obtain access to text messages (e.g., from a seized mobile phone) directing the front men to send or receive funds. If individuals other than the front men control the transactions, then the front men cannot be the true beneficial owners of the funds. Having been caught making a false statement, and vulnerable to prosecution for making a false statement, the front men have a choice. They may either cooperate with the prosecutor and identify the criminal controlling the transactions or risk imprisonment. If they cooperate and identify the criminal, the scheme unravels, and the prosecutor can go after the criminal orchestrating the transactions.

³² Smurfing involves structuring the funds into amounts below standard reporting thresholds.

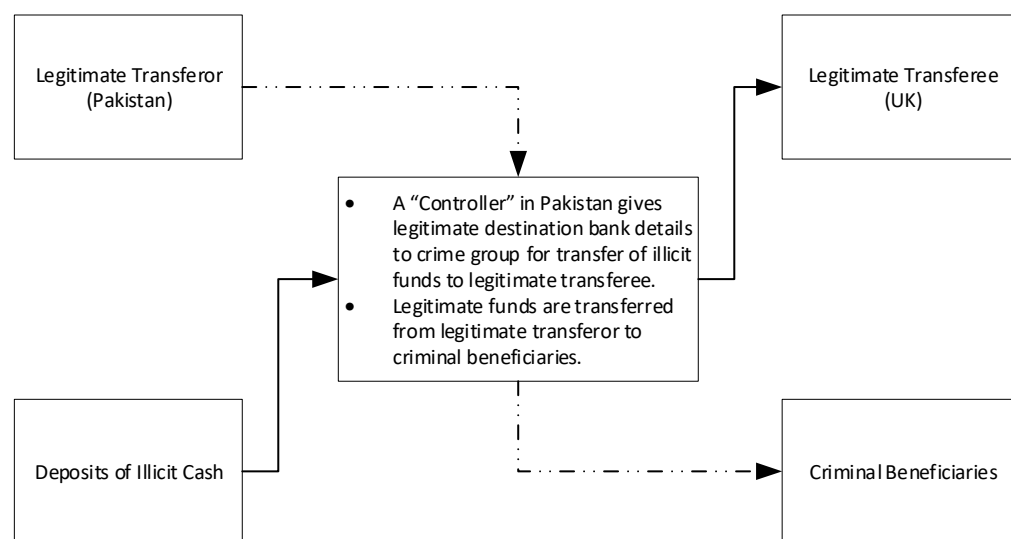


Figure 4. Money laundering via cuckoo smurfing.

3.3.6. Case 6: Invoice Manipulation

Suppose that criminals deposit USD 1 million in cash with a foreign company. The company invoices a sale of one million plastic buckets at USD 2 per bucket to a UK company, which sells the plastic buckets at the same price to legitimate purchasers (Murray 2016, p. 456). This creates a paper trail via the books and business records of the two companies that legitimizes USD 2 million of transactions.

However, while the UK company receives USD 2 million from the sale of the buckets, it only pays USD 1 million to the foreign company (Figure 5). The foreign company hides the discrepancy between the amount invoiced and the amount received by falsifying its accounting records. The excess profits of USD 1 million are paid via an intermediary to the criminals. This circuitous route hides the origin of the funds. In the absence of evidence of a predicate offense, it would be extremely difficult to prove money laundering.

Conventional AML regulations fail to address this type of scheme (Murray 2016, p. 456). In contrast, the APUNCAC Beneficial Owner Rule would require the bank clerks handling the cash deposits to obtain certification of beneficial ownership from the true beneficial owners for each cash transaction exceeding USD 3000. The Rule would also require the agent serving the intermediary to obtain certification of beneficial ownership from the true beneficial owners for each wire transfer exceeding USD 3000.

If front men falsely certify beneficial ownership of the funds, they become vulnerable to prosecution if a prosecutor manages to obtain access to text messages (e.g., from a seized mobile phone) directing the front men to deposit cash or send or receive funds. If persons other than the front men control the transactions, then the front men cannot be the true beneficial owners of the funds. Having been caught making a false statement and vulnerable to prosecution for making a false statement, the front men have a choice. They may either cooperate with the prosecutor and identify the criminal controlling the transactions or risk imprisonment. If they cooperate and identify the criminal, the scheme is unraveled, and the prosecutor can go after the criminal orchestrating the transactions.

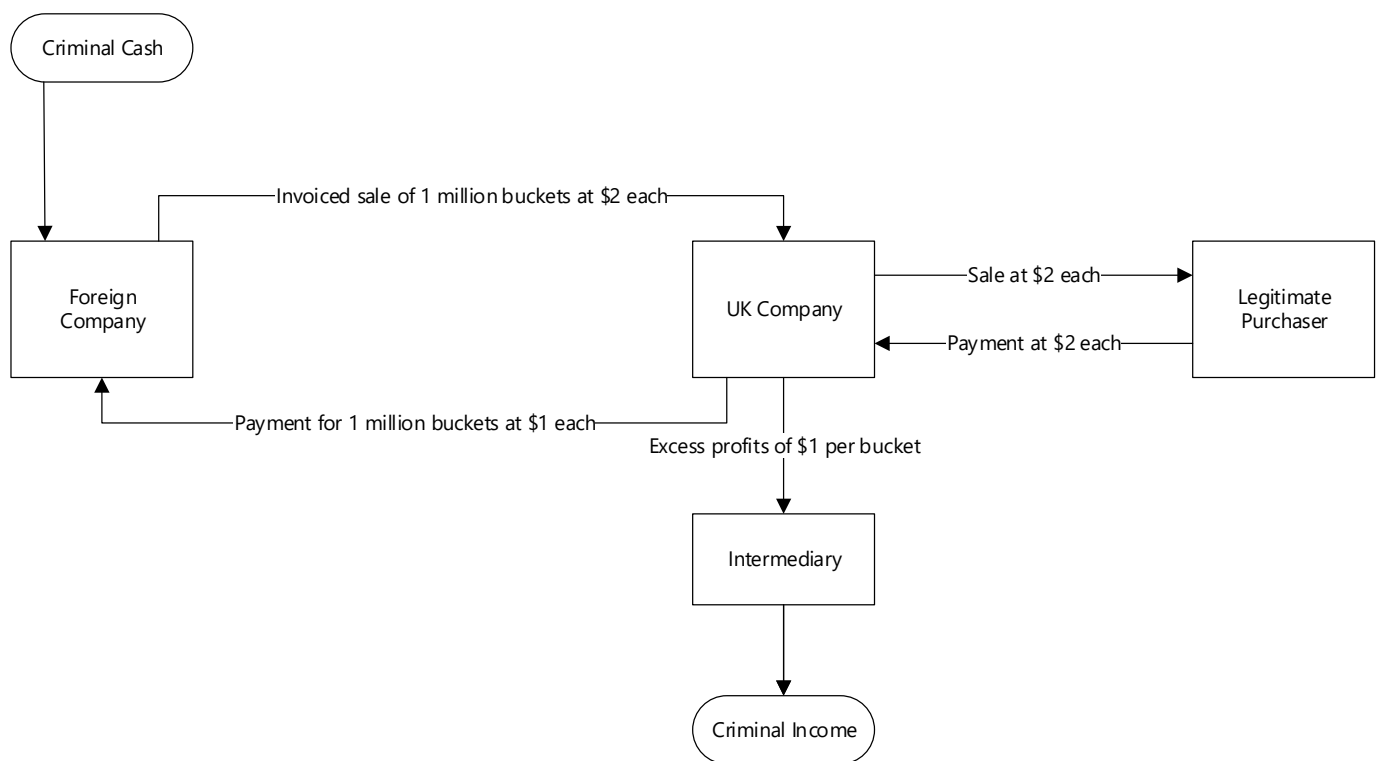


Figure 5. Trade-based money laundering via over-invoicing.

In addition, the Rule prohibits any person or entity from acting in a manner that seeks to evade or assists in evading the Rule, including the creation or use of false invoices, under-invoicing, or over-invoicing.³³ Each violation of this prohibition would be punishable by debarment, a fine not to exceed USD 250,000, or imprisonment not to exceed five years.³⁴ This prohibition would seek to deter the type of over-invoicing scheme described in the case example.

A prosecutor who utilized the APUNCAC Rule to leverage the cooperation of criminals involved in the transactions would then be able to obtain their witness testimony regarding the entire TBML scheme. In this way, a prosecutor could associate individual transactions with the TBML scheme, associate the scheme with the criminals who mastermind the scheme, and obtain convictions of the criminal masterminds.

3.3.7. Case 7: Illicit Flows in Bolivia

In certain countries, illicit activity and resulting illicit financial flows are tolerated by government regulators. In Bolivia, for example, illicit activity related to gold production, trade, and export is tolerated by the government. “Nearly all *rescatistas* and intermediary traders are informal, self-employed tradesmen who operate illegally”, with little government interference (Brugger et al. 2022, p. 12).

The government lowers formal requirements, reinterprets laws through decrees, removes incentives to comply with the law, and tolerates widespread evasion of laws and regulations regarding registration of legal entities, mining titles, production licenses, trading licenses, sales licenses, export licenses, environmental licenses, payment of taxes and duties, working conditions, labor laws, environmental regulations, and anti-money laundering regulations (see Brugger et al. 2022, pp. 10, 11, 14, 15, 17). Licensed export companies (*comercializadoras*) are permitted to export gold without ensuring adherence to all laws and regulations. “An AML expert noted that ‘most *comercializadoras* don’t care where the gold

³³ *Id.* art. 19(6).

³⁴ *Id.* arts. 40(2), 40(3).

comes from, only very few. I don't know if even one does it in a legally correct fashion, certifying that everything is in order'" (Brugger et al. 2022, p. 14). Consequently, informal, hazardous, exploitative, slave-like labor conditions are not uncommon and "illegally mined or smuggled gold can easily enter the formal value chain at any point before export" (Brugger et al. 2022, pp. 10, 14). "Channeling illicit gold or money flows into the Bolivian gold value chain is an almost risk-free activity" (Brugger et al. 2022, p. 14). The resulting financial flows are illicit.

Lax government regulation serves to maintain the political support of powerful labor cooperatives (Brugger et al. 2022, p. 17). Cooperatives favor loose regulation because members "benefit from lax controls that at least some exploit by engaging in illegal export practices, i.e., by creating illicit financial outflows" (Brugger et al. 2022, p. 17). Vigorous enforcement would threaten this source of income: "No one would be legally entitled to sell gold in Bolivia—all of them are illegals" (Brugger et al. 2022, p. 14). To avoid disruptions, "both sellers and exporters... make false statements regarding the legal provenance and origin of gold, frequently attributing gold shipments to unrelated cooperatives or submitting false copies of mining patents (*patente minera*)" (Brugger et al. 2022, p. 14).

False statements regarding provenance are enabled because there is no way to trace transactions to their source. This is facilitated by cash transactions. "Almost all financial transactions by gold collectors and intermediaries are conducted in cash, in violation of the 2015 decision by the National Tax Authority to prohibit cash transactions of more than Bs. 50,000 (about USD 7000)" (Brugger et al. 2022, p. 12). Cash transactions promote anonymity and undermine surveillance by Bolivia's anti-money laundering financial intelligence unit. "Since the *rescatistas* and intermediary traders are not registered, and since almost all transactions are conducted in cash, the UIF cannot perform any meaningful monitoring or control function" (Brugger et al. 2022, p. 15).³⁵ The result is a failure to verify provenance. "Since the chain of custody is often broken, this error-prone control of the 'origin' of gold regularly fails to verify provenance" (Brugger et al. 2022, p. 14). The government "remains toothless in detecting gold flows of illicit origin on account of the lack of due diligence by traders" (Brugger et al. 2022, p. 15).

The inability to trace provenance results in a failure of regulation. There is "no reporting of suspicious gold-related transactions from banks to the UIF unless an investigation into a certain client had already been initiated by law enforcement" (Brugger et al. 2022, p. 15). The result is that illicit gold exports are given an official stamp of approval. "Illicit gold consignments... are transformed into officially approved exports" (Brugger et al. 2022, p. 14). Thus, "the gold-trading sector offers ample opportunities for laundering money from the drug trade and other criminal activities" (Brugger et al. 2022, p. 11).

Application of the APUNCAC Rule would potentially address this type of situation.³⁶ The Rule would require informal local gold collectors (*rescatistas*) who buy small amounts of gold from small-scale miners and intermediary traders in regional gold-trading hubs who purchase gold from *rescatistas* to submit certification of beneficial ownership when making cash payments in amounts exceeding USD 3000. The Rule would require *comercializadoras* that purchase gold from *rescatistas* and intermediate traders to submit certification of beneficial ownership when making cash payments in amounts exceeding USD 3000. The Rule would require banks and non-bank financial institutions to submit certification of beneficial ownership when transmitting funds in amounts exceeding USD 3000 from foreign customers to Bolivian gold export companies.

³⁵ *Unidad de Investigaciones Financieras* (UIF) is Bolivia's financial intelligence unit, responsible for investigations of money laundering and financial crime.

³⁶ Bolivia is a member of the Financial Action Task Force on Money Laundering in South America [*Grupo de Acción Financiera de Sudamérica* (GAFISUD)], the South American FATF-style regional body. If the Financial Action Task Force (FATF) were to adopt the APUNCAC Rule, it is not unlikely that GAFISUD member states, including Bolivia, would also adopt the Rule. GAFISUD is modeled on FATF and has adopted the Forty Recommendations and the Special Recommendations against terrorism financing issued by FATF, the most widely recognized international standard for countering money laundering.

If front men falsely certified beneficial ownership of the funds (as payor or recipient), they would be vulnerable to prosecution if a prosecutor managed to obtain access to text messages (e.g., from a seized mobile phone) directing the front men to conduct transactions. If they cooperated and identified the person directing the scheme, the prosecutor could prosecute the person orchestrating the transactions. Awareness of this risk—and penalties including a maximum term of imprisonment of five years—would tend to deter violations of the Rule and deter money laundering.

By promoting accurate reporting of beneficial ownership, the Rule would facilitate verification of provenance and expose and deter illicit sourcing of gold from illegal mining operations employing workers in hazardous, exploitative, slave-like conditions. The resulting transparency, regulatory attention, and media attention could be expected to promote enforcement of labor laws, drive reform of the mining sector, promote human rights, and address rampant criminality and injustice. In sum, the Rule potentially offers a way forward in addressing illicit activity and illicit flows that are deeply institutionalized in informal practices driven by political calculations and expediency.

3.4. Digital Identification

Certification would occur via high-speed digital transactions, using digital identity certificates that electronically encode the same personal information contained in passports (see [IBM 2023](#)). The use of digital identity certificates would permit rapid electronic certification of beneficial ownership of funds subject to the APUNCAC Beneficial Owner Rule (see [Digicert 2022](#); [GlobalSign 2023](#)). Certification would utilize the same public key cryptographic technology as an ePassport to ensure the security of the data, prevent identity fraud, ensure that the information has not been altered, and ensure secure transmission to a Financial Crimes Enforcement Network (FINCEN) database modeled on the U.S. Treasury Department's FinCEN database. The use of digital identity certificates would provide assurance that the person who asserts beneficial ownership is, in fact, that person and not someone posing as that person ([Digicert 2022](#); [DocuSign 2022](#); [Entrust 2023](#); [IBM 2023](#); [IdenTrust 2023](#)).

The technology is the same technology that is utilized to ensure the security of credit card transactions. Transactions would be processed with the same speed and convenience, permitting millions of transactions per day. Improper authorization would cause a reversal of the transaction. Similar rules and procedures would apply to beneficial owner reporting.

Digital encryption, decryption, and tokenization execution times are measured in milliseconds, even when using outdated equipment. An analysis of an RSA encryption-based system using an outdated Windows 7 operating system and Pentium IV processor with 2 GB of RAM found computational times of 0.46 ms per Luhn Test, 0.46 ms per encryption, 0.47 ms per decryption, and 0.49 ms per tokenization ([Iwasokun et al. 2018](#), p. 291). The total computational time for these four tasks is less than 2 milliseconds. Digital beneficial owner certification would utilize the same technology.

3.4.1. Norway

A model digital system is Norway's BankID, which combines a secure digital identification (ID) and digital signature system that may be used to confirm a mobile payment, pay online via debit card, or sign official documentation ([BankID n.d.a](#); [Nikel 2022](#)). A white paper described the details ([BankID n.d.b](#)). The mobile version requires a mobile phone number, national ID number, and a mobile. A desktop version is available that does not require a mobile.³⁷ The BankID app simplifies the process and improves convenience. BankID offers a proof of concept, validated via real-world use since 2004, serving 4.3 million customers, 90 banks, and 9000 merchants ([PYMNTS 2022](#)). BankID will soon be replaced by mobile apps that will feature face or fingerprint biometric identification, improving security

³⁷ A thumb-sized device that is used to generate unique single-use passcodes for identity verification could be omitted with the adoption of biometric verification.

and offering a streamlined identity verification procedure (Macdonald 2022b). Sweden, Finland, Turkey, Slovenia, and Spain offer similar solutions (BankID n.d.c).

3.4.2. India

Aadhaar is the world’s largest biometric digital ID system. Approximately 96 percent of India’s 1.4 billion population is registered (Businesswire 2023). It has been described by World Bank Chief Economist Paul Romer as “the most sophisticated ID programme in the world” (Daijiworld News 2017). Citizens of India and resident foreign nationals are assigned a 12-digit unique identity number linked to biometric and demographic data collected by the government of India under the Aadhaar Act, 2016. The biometric information may include a photograph, fingerprints, or iris scans.

To enroll, residents complete an application form and present identification documents (Chin et al. 2015, p. 4). If an enrollee does not have identification documents, identification may be performed with the assistance of a person whose identity has already been verified who vouches for the identity of the enrollee (Chin et al. 2015, p. 4). The enrollee’s biometric data are recorded and entered into the database (Chin et al. 2015, p. 5).

The assigned Aadhaar number for an individual is connected to all biometric data collected during the enrollment process. A trained enrollment center employee photographs the enrollee, records the iris scans of the eyes, collects demographic information, and takes imprints of all 10 fingers. The demographic information includes the name, address, date of birth, and gender of the individual (Sathe 2011; Sharma 2011). Multiple biometric data are recorded in order to enable the inclusion of all residents in India. Fingerprints, for example, can be worn away by physical labor. Since many of the poor residents of India have occupations that require heavy physical labor, a fingerprints-only identification scheme would continue to disenfranchise many of them.

Each enrollee’s data is then uploaded to the Central Identification Data Repository (CIDR) for de-duplication. The term “de-duplication” refers to the process where the CIDR checks to determine whether or not the biometric data submitted already exists in the database. If no equivalent record exists, then a unique, randomly generated 12-digit number will be mailed to the enrollee (Mathew 2014; Sharma 2011). The unique identification number provides residents with the ability to clearly establish their identity when obtaining goods or services from any public or private organization.

(Chin et al. 2015, p. 5)

The implementation of Aadhaar demonstrates the feasibility of implementing a digital biometric ID system in the world’s most populous, largely rural nation, including areas posing significant barriers with limited access to technology and low levels of literacy.

3.4.3. China

In 2022, China implemented a digital ID system based on the national ID card system to access key public and private services online (Macdonald 2022a). The digital ID cards are now currently accepted in at least 15 major cities in the country (Macdonald 2022a). The digital ID card can be used by scanning a code on the user’s mobile phone (Macdonald 2022a).

3.4.4. Japan

Japan implemented a digital ID system and will require its use starting in 2024 to access public health insurance (Kageyama 2022; Mascellino 2022). Approximately half of Japan’s population has adopted the digital ID (Kageyama 2022; Mascellino 2022).

3.4.5. Indonesia

Indonesia, a country of 282 million people and the largest and fastest-growing digital economy in Southeast Asia, has implemented a biometric digital ID system. “More than 95 percent of the Indonesian population” has digital e-KTP ID cards “linked to a government database of citizen identities and biometrics” (Sumsuub n.d., p. 26). In 2022, 93.7 percent of mobile devices were utilized for verification purposes (Sumsuub n.d., p. 25). Indonesia will receive USD 250 million in funding from the World Bank to strengthen and expand its existing biometric digital ID system for accessing public and private sector services (Hersey 2023). The existing system is currently utilized to establish identity for a range of public and private services and by financial services providers to comply with know-your-customer (KYC) anti-money laundering (AML) regulations (Hersey 2023).

3.4.6. Russia

Russia plans to introduce a national digital ID system in 2024 (TASS 2019). In February 2023, Russian President Vladimir Putin approved the Russian Ministry of Digital Development’s plan to issue a draft order that would allow users to utilize a smartphone-based digital identity document as a substitute for a passport in certain identity-proofing situations (InterFax 2023). The plan follows an earlier agreement to allow biometric passport owners to obtain a digital ID.

The Digital Development Ministry and FSB earlier agreed on a similar technology to allow biometric passport owners to obtain Fan IDs entirely in the digital form through the ministry’s app, without applying to a Public Services Center in order to prove one’s identity. . . The owner’s identity is verified in this case with the help of their photo recorded on a chip in a biometric passport. (InterFax 2023)

Russia’s Minister of Digital Development, Maksut Shadayev, noted that the mobile application of digital ID permits a user to download a photo from the user’s biometric passport directly to a smartphone, then generate a QR code linked to the user’s government identity information that can be used for identity verification purposes (InterFax 2023). According to Shadayev, “The use of such an ID should allow using your smartphone instead of your original passport document ‘in 80% of cases in such day-to-day, simple situations’” (InterFax 2023). The “technology is already approved by FSB with regard to security and data protection requirements” (InterFax 2023).³⁸

3.4.7. Argentina

Argentina, the third most populous country in Latin America, has implemented a national digital ID system (Pascu 2020). Since 2009, Argentina has issued approximately 47 million digital IDs, covering almost the entire population of 46.4 million (Sumsuub n.d., p. 6).³⁹ The digital ID enables mobile identification via a mobile app (Pascu 2020) and “is now considered fully equivalent to traditional identity documents” (Sumsuub n.d., p. 6). Citizens may request a mobile ID by filing an application. Upon approval, a code is received to activate the digital National Identity Document (DNI) (Pascu 2020).

The Argentinian capital, Buenos Aires, will implement an improved digital biometric ID system for public and private sector use (Burt 2022). The system is designed to address flaws in the prior digital ID system and was expected to be operational no later than the first quarter of 2023 (Burt 2022).

3.4.8. Brazil

Brazil, the seventh most populous country in the world, has implemented a biometric digital ID system.

³⁸ The Federal Security Service of the Russian Federation (FSB) is the principal security agency of Russia.

³⁹ Issuance of digital IDs since 2009 exceeds the current population of 46.4 million because the latter figure does not include individuals who received digital IDs but are now deceased or have emigrated and are no longer nationals of Argentina.

In 2017, the Brazilian government enacted a federal law which established the National Civil Identification System (ICN or *Identificação Civil Nacional*). The ICN is composed of one centralized database, composed, mainly, of citizens' biometrics that had been collected by the Superior Electoral Court for electoral purposes. By the end of 2020, more than 120 million Brazilians had already completed their biometric registration, which represents more than half of Brazil's large population. (Garrote et al. n.d.)

Authentication is performed via the ICN system through the users' biometric data (Garrote et al. n.d.). By June 2022, 130 million users, equivalent to 80 percent of Brazil's population over 18 years old, were registered (Garrote et al. n.d.). A new form of identity cards incorporating QR codes was projected to be fully integrated no later than March 2023 (Sumsb n.d., p. 11). The rapid implementation of Brazil's digital ID system signals the emergence of digital ID in Latin America.

3.4.9. European Digital Identity

In 2024, the European Union (EU) will implement the European Digital Identity scheme, which is the EU equivalent of BankID (BiometricUpdate.com 2022). European Digital Identity is a digital identity wallet that will be available to all EU citizens and residents (European Commission 2022). It will enable EU residents to securely store digital identity credentials, conduct transactions requiring identity credentials, and sign documents electronically (European Commission 2022).

The proposed regulation would require each EU Member State to issue a European Digital Identity Wallet.⁴⁰ The proposed regulation specifies that wallets "shall enable the user to: (a) securely request and obtain, store, select, combine and share. . . the necessary legal person identification data. . . to authenticate online and offline in order to use online public and private services; (b) sign by means of qualified electronic signatures".⁴¹ The proposed regulation would require that digital identity wallets "ensure that the person identification data. . . uniquely and persistently represent the natural or legal person. . . associated with it".⁴² "Member States shall. . . include. . . a unique and persistent identifier. . . to identify the user".⁴³

The European Digital Identity system would pave the way for the implementation of the APUNCAC Rule by establishing an international operational and legal model for employing digital identity certificates to digitally sign and certify the type of self-certification of beneficial ownership that would be required by the APUNCAC Rule.

3.4.10. Africa

A World Bank study of African nations found that almost three-quarters of the countries covered have introduced digital IDs that employ biometrics to achieve deduplication and ensure that individuals are uniquely identified, and more are in the process of doing so (World Bank 2017, p. vi). Smartphone penetration and mobile internet coverage are expanding across the continent, with estimates suggesting that mobile penetration will rise from 50 percent to 64 percent by 2025 (Theodorou 2022). This enables countries across Africa to adopt digital ID systems and bypass the challenges of now-outdated paper-based credentials and identification schemes (Theodorou 2022).

Government policies have played a pivotal role in harnessing mobile technology to advance the implementation of digital ID systems in Africa. Government mandates to register prepaid mobile SIM cards against the users' national IDs have driven adoption of digital ID credentials (Theodorou 2022). The adoption of digital IDs has increased in direct

⁴⁰ Commission Proposal for a Council Regulation Amending Regulation 910/2014 as regards Establishing a Framework For a European Digital Identity, art. 1(7)(1), 2021/0136 (COD) [hereinafter eIDAS 2].

⁴¹ eIDAS 2, art. 1(7)(3).

⁴² *Id.* art. 1(7)(4)(e).

⁴³ *Id.* art. 1(12)(2).

proportion to the rapid increase in demand for mobile subscriptions involving SIM cards registered in user names (Theodorou 2022). A World Bank study found that the primary reason people in developing countries apply for an ID is to buy a new SIM card or to register their existing SIM card against their ID to avoid having it deactivated by a government-imposed deadline (where mandatory SIM registration is enforced) (Theodorou 2022).

In Nigeria and Tanzania, authorities license mobile network operators (MNOs) to act as official ID enrollment partners, effectively leveraging their nationwide presence to accelerate citizen enrollment onto the national digital ID platform, thereby supporting the inclusion of several million people who had been previously unregistered (Theodorou 2022).

Digital ID rollouts increasingly involve the capture of an individual's biometrics (fingerprints, iris, face, voice) to avoid duplication of records and ensure that individuals are uniquely identified (Theodorou 2022). This is facilitated by new smartphone technologies that can be used to capture individual biometric attributes during ID enrollment (Theodorou 2022). For example, smartphone cameras coupled with machine learning and AI software are being used for identity verification and authentication by companies such as Element.inc and Tech5 (Theodorou 2022).

In January 2014, 55 African Union (AU) heads of state endorsed the SMART Africa Manifesto (SMART Africa Alliance 2020b). The Manifesto commits AU states to accelerated adoption of information and communications technology (ICT) to promote socio-economic development. In 2020, the 32 African member countries of the SMART Africa Alliance published a "blueprint" for establishing technical standards, rules, and requirements to achieve mutual recognition and interoperability of national digital ID systems across the African continent (SMART Africa Alliance 2020a).

The blueprint emphasized that "Digital Identity systems are at the heart of Africa's digital transformation agenda" (SMART Africa Alliance 2020a, p. 3). The SMART Africa blueprint seeks to "facilitate and enable future pan-African interoperability of ID systems" (SMART Africa Alliance 2020a, p. 3). Interoperability requires the establishment of technical standards to enable cross-border and interjurisdictional recognition of digital IDs among relying parties and identity providers (SMART Africa Alliance 2020a, pp. 3, 33). The blueprint recommended the creation of a SMART Africa Trust Alliance (SATA) to provide a governance structure and technical framework to achieve common technical standards, rules, and mutual recognition across national ID systems (SMART Africa Alliance 2020a, p. 4). The objective is "to create an effective framework for safe and trusted cross-border digital interactions" (SMART Africa Alliance 2020a, p. 4). This will involve the establishment of digital identity systems that identify "a natural or legal person" associated with each ID (SMART Africa Alliance 2020a, p. 6).

The draft African Union Continental Data Policy Framework seeks implementation of a Digital ID to facilitate cross-border digital transactions (AU 2021, Annex 3 Section 5.3.1.3 Digital ID). Digital identification is defined as "a set of electronically captured and stored attributes and/or credentials that uniquely identify a person enabling the distinction of one individual from another" (AU 2021, Annex 3 p. 60).

"Individuals who hold an ID from a national system will be able to obtain an interoperable digital credential for legal identity (IDC-ID)" (AU 2021, p. 2). The IDC-ID will enable the holder of the IDC-ID to present credential data signed via a digital signature, proving the authenticity of the data.

AU Member States have the freedom to select how they want to issue this digital credential. It may be stored in a purely digital format on a smartphone application, a cloud-based server, a smartcard, or a link to the digital representation may be established using a one- or two-dimensional barcode on a paper document (printed on paper, plastic card). Member States can also decide to reuse this standard to represent identity data at the national level. (AU 2021, p. 2)

A specialized technical committee report described technical options to enable the holder of an IDC-ID to authenticate his identity. One option is to utilize a personal digital wallet modeled after the European Digital Identity Wallet (AU 2021, Annex 2, pp. 24–25).

After completing an identity-proofing process, a wallet could be used to store credential data in a digital format. Using public key infrastructure, the data could then be presented as needed or desired to a relying party who could rely on the authenticity of the data and verify that the data are authentic (AU 2021, Annex 2, pp. 23–24). A second option is to establish a continental federation of ID credential providers, issue an IDC-ID to each user, and establish a continental exchange for participating credential providers and relying parties for the purpose of authenticating individual users (AU 2021, Annex 2, p. 25). A third option is to utilize digitally signed credentials to authenticate legal identity data (AU 2021, Annex 2, p. 26).

The SMART Africa blueprint established a three-phase implementation timeline. Phase 2, involving implementation of the framework and adoption of technical specifications for the IDC-ID, is to be completed in 2023–2024 (AU 2021, Annex 2 pp. 27, 29). Phase 2 will include the development of standards to achieve cross-border interoperability of the IDC-ID, including cryptographic encryption and signatures and verification protocols for online and offline use cases (AU 2021, Annex 2 p. 29). A model IDC-ID app will be developed and piloted by a group of AU Member States to test verification, privacy, and security features and cross-border interoperability of the credential (AU 2021, Annex 2 p. 29).

The drive to establish interoperable digital identity systems is driven by the need to address barriers in the delivery of public and private services: “Digital identity represents the backbone of Africa’s transformation into a digital single market, as it is a basic building block for access to both public and private services” (SMART Africa Alliance 2020a, p. 13).

3.4.11. Global Adoption

A recent report forecasts that more than 3 billion people globally will be equipped with a government-initiated mobile ID app by 2024 (Theodorou 2022).

Developments have been most dramatic in Southeast Asia, where biometrically based, digital forms of ID have reached most of the adult population in Bangladesh, India, Indonesia, and Pakistan. The new systems are gradually being integrated into the delivery of public and private sector goods and services, especially in India and Pakistan. (World Bank 2017, p. v)

Digital identification systems have also been implemented in Latin America, including Chile, Peru, Mexico, and Brazil (Barbosa et al. 2020).

3.4.12. MOSIP

In recognition of the need to support the implementation of affordable digital identity systems across developing nations, the Gates Foundation funded the Modular Open Source Identity Platform (MOSIP) (MOSIP n.d.a). MOSIP “is a unique, universal, and progressive digital identity system which is also an open source platform that nations can [freely use to] build their own identity systems” (MOSIP n.d.b). Individual users receive a unique government identifier for identity assertion and verification. The digital ID can then be used to access a wide variety of government and private services. MOSIP seeks to provide a freely available, open-standard, world-class infrastructure and platform to assist government agencies in building and implementing secure, interoperable, national digital identity systems (MOSIP n.d.a). Development is based at the International Institute of Information Technology, Bangalore (IIIT-B) (MOSIP n.d.a). Over 76 million users are registered on MOSIP-based digital ID systems (MOSIP n.d.a).

3.4.13. ID2020

ID2020 is a public–private initiative and consortium that seeks to facilitate the global implementation of digital ID legal identity technology for all people, including the world’s most vulnerable populations, consistent with the United Nations Sustainable Development Goals. In May 2016, over 400 attendees met at the United Nations Headquarters in New York, the inaugural ID2020 summit, to address the Sustainable Development Goal of equipping the world’s population, including 1.5 billion people living without any form of

recognized identification, with a digital identity (ID2020 2016). Experts in authentication, cryptography, telecommunications, and transaction processing joined with 11 UN agencies, government representatives, and representatives of technical standards bodies to identify solutions (ID2020 2016; Schwartz 2016).

The September 2018 summit focused on defining what constitutes a “good” digital ID. Sponsors for the event included the United Nations Office of Information Communications Technology (OICT), the United Nations High Commissioner for Refugees (UNHCR), the International Telecommunication Union (ITU), and the Consulate General of Denmark in New York (UNHCR 2018). In September 2019, ID2020 launched a digital identity program in collaboration with the government of Bangladesh, the Gavi vaccine alliance, and partners in academia and humanitarian relief to establish digital identity in combination with vaccination and immunization records (Burt 2019). The program will include biometric enrollment and digital ID for infants when they receive routine immunizations, offering a model that can be replicated in other countries (Burt 2021).

3.4.14. Digital ID Summary

These developments signal the growing adoption and implementation of digital biometric ID systems worldwide. Adoption is proceeding at a rapid pace in China, Japan, and Russia, the Member States of the EU, other countries, including Argentina, Bangladesh, Brazil, Chile, India, Indonesia, Pakistan, Peru, and Mexico, and members of the African Union.

The public and private impetus to adopt digital ID technology and digital ID systems and establish interoperable systems that facilitate cross-border digital transactions suggests that the required technology and systems will be increasingly accessible to and adopted by a global population, including individuals in Africa and Asia who traditionally lack access to technology and national identity systems. While the U.S. currently does not employ a national identity system, the adoption of digital ID systems in Europe, Asia, Latin America, and Africa suggests that it would be feasible and practical.

The adoption of digital ID systems has been described as a breakthrough, with “emancipatory potential” to empower marginalized groups, including refugees, women, and others who lack paper IDs or have been excluded from a national ID system (Guliani 2022, pp. 92–94). Digital identity enables access to social and medical services, police protection, and financial benefits (Guliani 2022, pp. 93–94). Significantly, digital ID systems can be implemented separately from national ID systems. The adoption of digital ID systems is increasingly supported by policymakers, researchers, and practitioners working in aid and migration management (Guliani 2022, p. 92). United Nations High Commissioner for Refugees (UNHCR), the Red Cross, the UN Migration Agency, and global government agencies have expressed interest (Guliani 2022, p. 92).

3.5. Identity Proofing

The acquisition of a digital ID would be preceded by a one-time identity-proofing process analogous to the identity-proofing process required to obtain a passport. In cases where a person is not able to obtain a passport, identity proofing for the purpose of obtaining a digital ID could be accomplished via biometric identification without a passport. In most cases, however, existing passport identification systems could be utilized to establish a person’s identity for the purpose of obtaining a digital ID.

Currently, 171 countries worldwide, including EU countries, have issued digital biometric ePassports that utilize fingerprint or face recognition technology to prevent identity theft (ReadID 2023). The same technology could be utilized to generate a secure digital certificate that would identify a person asserting beneficial ownership, prevent identity fraud, and permit high-speed certification of beneficial ownership, minimizing transaction friction.

Biometric identification would enable authorities to identify criminals who attempt to steal the identities of legitimate individuals. Since criminals would not be able to attach the

correct biometric information to the ePassport information, they would be forced to attach their own biometric information. The mismatch and the fraud would become obvious when authorities match the information to the FINCEN database containing the proper information for each legitimate person. Biometric identification is a strong antidote to identity theft, and the prevention of identity theft is a strong argument in favor of biometric identification. A person who is hesitant may, when faced with the threat of identity theft, choose to protect his identity via biometric identification.

The identity-proofing procedure would involve two steps. In step one, each person who meets a specified income and asset threshold would apply for an ePassport.⁴⁴ In step two, each person would use his/her ePassport to obtain a digital identity certificate that contains, in a digital format, the same information as an ePassport. Operational implementation of the APUNCAC Beneficial Owner Rule would involve electronic submission of the digital identity certificate at the point of certifying beneficial ownership (i.e., when a covered transaction occurs). The digital format would permit secure, high-speed, high-volume transmission of the identity information and would obviate the need to review paper documents such as an ePassport.

To prevent corruption of the identity-proofing process, the process may be performed via random assignment to a qualified trust service provider that would perform supervised remote identity proofing (SRIP) (see [NIST n.d.b](#)).⁴⁵ “Remote identity proofing methods provide the possibility to identify persons without needing an actual physical presence in the same room”, although best practice would involve a monitored kiosk ([ENISA 2021](#), p. 7). Qualified Trust Service Provider (QTSP) staff identities would be verified via biometric identification, and staff would be vetted via criminal background checks performed within the past year. Random assignment would prevent criminals from identifying and bribing the specific trust service providers assigned to verify the identity of applicants for digital identity certificates. To ensure the integrity of the proofing process, SRIP would be combined with biometric authentication methods that uniquely identify individual applicants (see [Kursun et al. 2018](#); [NIST n.d.a](#)). This form of SRIP would adhere to the strongest NIST standards for authentication.

EU Member States signaled approval of strong remote identity-proofing procedures via Regulation 910/2014 on electronic identification and trust services for electronic transactions conducted within the EU (see [ENISA 2021](#), p. 4).⁴⁶ Regulation 910/2014 paves the way for remote identity proofing (see [ENISA 2021](#), p. 8).⁴⁷ Regulation 910/2014 was incorporated by reference into the 5th Anti-Money Laundering Directive (5AMLD) for

⁴⁴ The income and asset threshold would be tailored by each nation; high-income countries would set higher thresholds than low-income countries. Note that each State Party to APUNCAC may tailor the identity-proofing process to align with existing national identity systems. However, best practice would involve biometric identity proofing and ePassports. The inconvenience of obtaining an ePassport would be no different than the inconvenience of obtaining a European Digital Identity or an African digital ID. The requirement would mainly apply to individuals who have the wealth and propensity to travel abroad and, therefore, are likely to apply for an ePassport regardless of the Rule. An alternative procedure to obtain a digital ID, using biometric information, may be implemented for individuals who are unable to obtain an ePassport. In addition, an exception to the ePassport requirement could be granted for persons who certify that they will not engage in covered transactions. This certification would be entered into the FINCEN database and would flag any covered transaction involving the named person. If that person's identity was stolen by a criminal for the purpose of conducting illicit transactions, the flag would halt the transaction and trigger an investigation.

⁴⁵ A Qualified Trust Service Provider (QTSP) must comply with strict requirements under the EU's eIDAS regulation that ensure the validity and security of the certificates, keys and signatures that are the foundation of identity proofing and the creation of digital identity certificates bound to applicant identities. QTSPs undergo an independent assessment and regular audits to ensure that they continue to adhere to the QTSP requirements as defined by eIDAS.

⁴⁶ Council Regulation 910/2014 on Electronic Identification, 2014 O. J. L 257/73.

⁴⁷ *Id.* art. 24(1)(d). The National Institute of Standards and Technology (NIST) standard SP 800-63A § 5.3.3.2 provides for supervised remote identity proofing. The standard seeks to promote, for identity-proofing processes that are performed remotely, a level of confidence and security comparable to the level for in-person identity-proofing processes. SP 800-63A is treated as an international standard.

the purpose of identifying customers and verifying customer identity.⁴⁸ Eleven European supervisory bodies accept methods for remote identity proofing (ENISA 2021, p. 6). Most EU Member States allow some form of remote identity proofing (see ENISA 2021, Figure 7, Table 4). In sum, most EU Member States support the use of remote identity-proofing procedures for the purpose of authenticating the identity of a party involved in a transaction. Significantly, the EU's General Data Protection Regulation (GDPR) would not block the necessary data collection and storage.⁴⁹ "GDPR does not forbid data controllers to store personal data if such storage is lawful and necessary" (ENISA 2021, p. 40).

Individuals who fall below the FINCEN income and asset threshold and are not required to obtain a digital identity certificate would be unlikely targets of criminal impersonators. A criminal who stole the identity of a person who falls below the threshold would attract attention if he conducted frequent high value cash transactions, international transactions, or transactions involving high-risk jurisdictions such as BVI, the Caymans, or Panama. For example, a criminal could steal the identity of a rural farmer, but a rural farmer does not typically engage in these types of transactions. A criminal who poses as a rural farmer but conducts this type of transaction would attract attention and would be readily flagged for investigation and prosecution. After the true farmer disavows the transactions, the criminal scheme would be exposed. For this reason, it is unlikely that criminals would seek to steal the identities of individuals whose income and assets fall below the threshold.

3.5.1. What Is an ePassport?

An electronic passport, or ePassport, is the same as a traditional passport book with the addition of a small, embedded integrated circuit (or chip). In the United States and many other countries, the chip is embedded in the back cover. The chip stores:

- The same data visually displayed on the data page of the passport;
- The passport holder's picture stored in digital form;
- The unique chip identification number;
- A digital signature to detect data alteration and verify signing authority;
- Additional data, as defined by specific issuing governments. (Smart Card Alliance 2009)

Standards for the ePassport have been established by the International Civil Aviation Organization (ICAO) and are followed by all countries implementing ePassports.

3.5.2. How Is an ePassport Obtained?

An ePassport is obtained via the standard passport application procedure. Countries that have adopted the ePassport will automatically issue an ePassport, instead of a traditional passport, upon approval.

3.5.3. How Many Countries Use ePassports?

Adoption of ePassports is accelerating. Of 196 countries in the world, 171 now use ePassports, including all European Union countries and most other major countries (ReadID 2023). Over 1.2 billion e-passports were in circulation in 2021 (Thales 2023).

3.5.4. Are ePassports from All Countries the Same?

No. All ePassports follow the common ICAO standard. However, countries implement ePassport programs according to their specific policies and may implement different options specified in the standard. This results in differences among country implementations of

⁴⁸ Council Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU, art. 1(8)(a) [amending art. 13(1)(a)], 2018 O. J. L 156/43 [hereinafter 5AMLD].

⁴⁹ Council Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 6(1)(c) and 6(1)(e), 2016 O. J. L 119/1 [hereinafter GDPR].

ePassports even though they all conform to the ICAO specification. If fingerprint images are not included, independent service providers are available and may be utilized to obtain, store, and link fingerprint images to each person's ePassport information.

3.5.5. Are ePassports More Secure than Traditional Passports?

Yes. The ePassport uses advanced digital and physical security technologies that significantly increase the difficulty of passport forgery and provide significantly higher levels of security.

3.5.6. What Security Measures Are Built into an ePassport?

The technology embedded in an ePassport involves a secure microcontroller utilizing advanced cryptography to detect attacks. When the ePassport is personalized and issued, the data which have been written to the chip are signed by the issuing authority using the country signing key: a secure, digital, cryptographic key that permits easy detection of forgery or alteration. Once manufactured and personalized, no information can be changed ([Smart Card Alliance 2009](#)).

3.5.7. Does Reading an ePassport Compromise the Security of the Information?

No. Reading the electronic data in an ePassport does not compromise the security of the information. The access control mechanism denies access to the chip contents unless the inspection system can prove that it is authorized to access the chip. These access control mechanisms prevent skimming of the chip data and eavesdropping the communications between an ePassport and the inspection system. ([ICAO 2023a](#)).

3.5.8. How Does a Border Official Determine That an ePassport Is Valid?

ICAO has established a Public Key Directory (PKD). Each country that issues ePassports digitally signs the data with the corresponding country signing keys. Each country publishes its public key in the PKD, permitting border officials to check the validity of the ePassport's electronic information. However, cryptographic techniques ensure that knowledge of the public key is insufficient to sign, forge, or alter information in an ePassport. The process of ePassport validation involves verification of the digital signature on the chip of an ePassport to confirm its authenticity and integrity. The process of ePassport validation does not require or involve the exchange of personal information of passport holders. By authenticating the chip of an ePassport, border control authorities can confirm that:

- The ePassport held by the traveler was issued by a bona fide authority;
- The biographical and biometric information endorsed in the document at issuance has not subsequently been altered; and
- If active authentication and/or chip authentication is supported by the ePassport chip, the electronic information on the chip is not a copy (i.e., a clone). ([ICAO 2023b](#)).

The authentication of the electronic component of the ePassport (i.e., the chip) contributes to confidence in the information contained in the ePassport. Border control authorities can confidently rely on the information on the chip.

3.6. Dual Paired Certification

Certification would be required by the beneficial sender as well as the beneficial recipient. The paired certifications would be obtained twice: by the personnel assisting with the transmission of the funds, as well as the personnel assisting with the receipt of the funds.⁵⁰ Thus, two paired sets of beneficial owner information would be transmitted to FINCEN for each transaction. The information must match; otherwise, the transaction would be reversed. The dual requirement to submit a paired set of beneficial sender and beneficial recipient information would serve to deter willful noncompliance by financial

⁵⁰ APUNCAC arts. 21(2)(a)(H), 21(3)(a)(viii), 21(3)(b)(viii), 22(1)(a)(G), 30(b).

service personnel or beneficial owners because noncompliance by either party (sender or recipient) would be obvious and would cause the transaction to fail.

A successful attempt to subvert the Rule would require a conspiracy among four parties: the beneficial sender, the financial service personnel assisting the beneficial sender, the beneficial recipient, and the financial service personnel assisting the beneficial recipient. In principle, the transaction should be halted or reversed by the financial personnel if the required certifications do not match. However, reversal of the transaction assumes that the financial service personnel are not complicit and, when notified of a mismatch, notify the customer that the transaction is in violation of the Rule and funds will not be released.

A false statement by either the sender or recipient would potentially implicate both the sender and the recipient in a criminal conspiracy. Each party would have a vested interest in ensuring that the respective counterparty submitted a secure, verified, accurate digital identity certificate and certification of beneficial ownership.

If, for example, a corrupt politician sought to transmit funds offshore to a Panamanian front account for which he was, in fact, the true beneficial owner, he and any front man would be guilty of a criminal conspiracy to hide the identity of the true beneficial recipient, in violation of the APUNCAC Beneficial Owner Rule. Front men who previously operated with impunity (because there is currently no requirement to self-certify beneficial ownership) would, under the Rule, need to think twice about whether the small financial rewards were worth the risk of arrest, extradition, trial, and imprisonment for making a false certification of beneficial ownership.

Financial service personnel in recalcitrant jurisdictions or employed by a recalcitrant financial service institution who sought to ignore the Rule and decline to submit the required beneficial owner certifications would find that the transaction would be halted (or reversed) because one-half of the required matching certifications would be missing. If, nonetheless, the transaction was completed in violation of the Rule, all four parties would then be implicated in a criminal act and subject to criminal penalties, including possible arrest, extradition, debarment, fines, and imprisonment. This prospect would tend to deter noncompliance. The risks could easily be avoided by declining to participate in any risky transactions. This would, from the standpoint of anti-money laundering authorities, be the desired outcome.

3.7. AML

The APUNCAC Beneficial Owner Rule would fight money laundering by deterring actions by financial service personnel that support and promote money laundering but are currently legal. Currently, it is legal for financial service personnel to process a series of transactions involving illicit funds that serve to obscure the origin of the funds if the personnel are unaware of the illicit origin of the funds. To ensure that the illicit nature of the funds is obscured, criminals may substitute front men who serve as the nominal senders and receivers on the sending and receiving accounts. The use of front men obscures the identities of the true beneficial owners who control the transactions (see Sections 3.9 and 3.10).

In contrast, implementation of the Rule would create two possibilities. One possibility is that the true beneficial owners—i.e., the criminals controlling the transactions—identify themselves, making an investigator's task of tracing illicit funds simple. The second possibility is that the true beneficial owners substitute front men. However, the Rule requires the front men to make certifications of beneficial ownership that are demonstrably false. Having committed the crime of making false certifications, the front men would be vulnerable to prosecution, as outlined above. This vulnerability would encourage cooperation with prosecutors. Cooperation would elicit information implicating anyone who directed the front men. Prosecutors would gain sufficient leverage to pursue those individuals. The threat of prosecution would, in turn, elicit information implicating anyone controlling the transactions, i.e., the criminals manipulating the transactions.

The Rule would fight money laundering by creating a credible threat to anyone involved in money laundering. That threat currently does not exist or is very weak. The

establishment of corporate beneficial owner registries does not establish a credible threat to money launderers because criminals identify and exploit numerous loopholes. Criminals can avoid the threat posed by corporate beneficial owner registries by selecting jurisdictions where registries do not exist, selecting vehicles such as trusts or investment funds that are not covered by corporate registries, selecting property such as virtual assets that are not covered by corporate registries, using crypto mixers to obscure the origin of illicit funds, or substituting front men who pose as beneficial owners.

In contrast, implementation of the proposed APUNCAC Beneficial Owner Rule would create a credible threat of prosecution: the threat that a prosecutor might obtain text messages directing a front man to send or receive funds, utilize the information to apply pressure to anyone involved in the transactions, extract incriminating information, and prosecute the criminals controlling the transactions. That threat does not currently exist because there is no existing requirement for the true beneficial owner to self-certify beneficial ownership at the point when a transaction occurs. In the absence of any legal requirement to self-certify beneficial ownership at the point when a transaction occurs, no crime is committed when financial service personnel unwittingly process transactions involving illicit funds. If no crime is committed, then front men have no reason to fear prosecutors and no reason to stop their participation as front men who effectively disguise the true beneficial owners controlling transactions involving illicit funds. In contrast, the implementation of the Rule would cause front men to commit a crime whenever they make false certifications regarding beneficial ownership. Implementation of the Rule would alter the cost–benefit calculations of every front man and every criminal involved in directing and controlling transactions involving illicit funds. This could be expected to reduce money laundering, perhaps dramatically.

In addition, detection of money laundering would likely improve with implementation of the Rule, because failure to submit beneficial owner certification would create a red flag that would attract attention from investigators. In contrast, there is no existing requirement to submit beneficial owner certification and, therefore, there is no red flag.

Under the existing regime, prosecution is difficult because prosecutors must prove the illicit nature of funds. Therefore, deterrence is weak. Implementation of the Rule would make prosecution easier because there would be no need to prove the illicit nature of funds. This would improve deterrence (Figure 6).

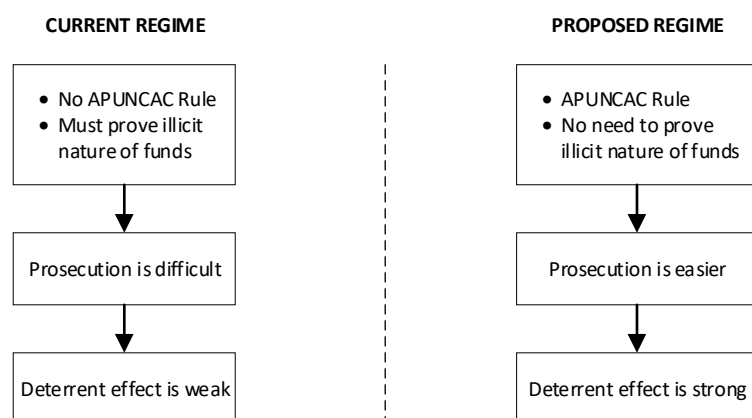


Figure 6. Prosecution is easier and deterrent effect is stronger with APUNCAC Rule.

3.8. TBML and IVTS

A question that arises is how the proposed Rule prevents organized crime networks from implementing sophisticated schemes where invoiced quantities and values are manipulated to hide trade-based money laundering (TBML). The Rule addresses this type of money laundering (see Section 3.3.6, above). A second threat is posed by trust-based *hawala* schemes and informal value transfer systems (IVTS) that accomplish the transmission of value across borders with no cross-border transfer of funds. The Rule also addresses this

type of money laundering. Both types of money laundering would be greatly curtailed if the flow of illicit funds channeled into and out of these schemes is curtailed. If the faucet is turned off and the drain is plugged, the flow of illicit funds through the system would be greatly reduced. Application of the Rule to *hawala* illustrates how the Rule would operate to stem the flow of illicit funds.

The key feature of *hawala* is that it operates outside the international banking system. Since *hawala* operates outside the international banking system, it may be abused for the purpose of money laundering.

Hawala is a popular informal system that accomplishes long-distance transfer of money without the movement of physical currency or telegraph or computer network wire transfers between banks. *Hawala* relies instead on the performance and honor of an enormous worldwide network of money brokers known as *hawaladars*. Most *hawaladars* are small businessmen who provide *hawala* services as a sideline operation.

The *hawala* system bypasses the formal banking system. A customer gives a local *hawala* broker a sum of money. The broker contacts a distant *hawala* broker who agrees to pay the sum to the intended recipient. To receive the sum, the recipient must provide a password that is communicated by the sender to the recipient. Each *hawala* broker maintains an accounting ledger to keep track of the amounts received from and owed to other brokers. These debts are settled through any form of payment that is acceptable among the *hawaladars*. *Hawala* brokers profit from customer commissions and favorable international settlements that are unencumbered by the conventional banking system's hefty foreign exchange transaction fees.

The unique feature of the system is that no promissory instruments are exchanged between the *hawala* brokers; the transaction takes place entirely on the honor system. As the system does not depend on the legal enforceability of claims, it can operate even in the absence of a legal and juridical environment. Trust and extensive use of connections are the components that distinguish it from other remittance systems. *Hawaladar* networks are often based on membership in the same family, village, clan, or ethnic group, and cheating is punished by ex-communication, "loss of honor", and resulting economic hardship.

Hawala is attractive to customers because it provides fast and convenient transfer of funds, typically at a far lower commission than the fees charged by banks. Its advantages are most pronounced when the receiving country applies unprofitable exchange rate regulations or when the receiving country's banking and legal system permits this type of informal transaction (e.g., Afghanistan, Yemen, Somalia). In some parts of the world, *hawala* is the most practical option, even for legitimate fund transfers. However, the *hawala* system can be used for money laundering because it operates outside the traditional banking system's regulations and legal requirements for collecting and verifying customer identity information. (Yeh 2020c, p. 452)

How would the proposed Rule be applied to *hawala* schemes?

Regarding *hawala*-based transactions, the APUNCAC reporting requirement would require each *hawaladar* to obtain, and submit to FINCEN, certification of beneficial ownership of funds paid to, or paid out by, a *hawaladar*; in an amount exceeding USD 3000.⁵¹ If the beneficial owner is a customer who is physically present, certification would be demanded from the customer. Other-

⁵¹ Assuming that the beneficial owner was a national of a State Party to APUNCAC and assuming a transaction in currency or involving a bank draft or bearer instrument. APUNCAC, art. 30(i). Alternatively, assuming that a *hawaladar* is within the jurisdiction of a State Party and assuming a transaction in currency or involving a bank draft, bearer instrument, negotiable instrument, wire transfer or money order. *Id.* art. 30(iii).

wise, a *hawaladar* would be required to contact the beneficial owner to obtain a digitally signed certification that the purported beneficial owner is indeed the true beneficial owner.

The APUNCAC reporting requirement also applies to transfers in currency; therefore, the transfer of currency from one *hawala* client to an end client would have to be reported to FINCEN.⁵² The sender would have to provide a digitally signed certification that he is the beneficial owner of the source funds. The recipient would have to provide a digitally signed certification that she is the beneficial owner of the funds received from the sender. The certifications would state that the funds do not involve the laundering of funds obtained illegally or through criminal activities and would acknowledge that criminal penalties apply if false or misleading information is provided.

A *hawaladar* who lacks internet access but wishes to offer *hawala* services would be limited to transaction amounts under USD 3000 because the APUNCAC reporting requirement would require the use of a broadband-enabled mobile phone, tablet, or computer to report transactions in excess of USD 3000. A *hawaladar* who wishes to offer *hawala* services in amounts exceeding USD 3000 would require access to the internet. Typically, however, such *hawaladars* already have internet access, even in developing countries in Africa, through a mobile broadband network.⁵³ It is unclear whether any *hawaladars* who currently engage in transactions exceeding USD 3000 lack Internet access and would be forced to curtail their business in response to the implementation of the APUNCAC reporting requirement. In any case, there would be a significant public benefit of implementing the APUNCAC reporting requirement. The requirement would be expected to reduce criminal activity, corruption, and impunity that serves to perpetuate poverty and inequality among the poorest of the poor in developing countries.

APUNCAC addresses the possibility that a criminal might employ front men to transmit illicit funds using mobile payment solutions in combination with *hawala*, to obscure the origin of illicit funds. The APUNCAC reporting requirement applies to this type of transaction (a) at the point when a customer pays a *hawaladar*, and (b) at the point when a *hawaladar* pays the end client, assuming that a *hawaladar* is within the jurisdiction of a State Party, and assuming a transaction in currency, or involving a bank draft, bearer instrument, negotiable instrument, electronic fund transfer or money order.⁵⁴ (Yeh 2020c, pp. 459–60)

⁵² *Id.* art. 30(i).

⁵³ By 2022, 3G mobile broadband network coverage reached 95 percent of the world's population (ITU 2022, p. 19). ITU, 2022, *Measuring Digital Development: Facts and Figures 2022*, Geneva: ITU. By 2021, 3G network coverage exceeded 80% of the sub-Saharan African population (GSMA 2022, Figure 14). GSMA, 2022, *The State of Mobile Internet Connectivity 2022*, London: GSMA. In 2016, more than 80% of citizens in Kenya and Nigeria had a mobile phone subscription (Hasbi 2020, p. 3). Hasbi, Maude, and Antoine Dubus, 2020, "Determinants of Mobile Broadband Use in Developing Economies: Evidence from Sub-Saharan Africa", *Telecommunications Policy* 44: 1–28, <https://doi.org/10.1016/j.telpol.2020.101944>. In Tanzania, 77% of citizens below the poverty level owned a mobile phone (Hasbi 2020, Table 2). In Nigeria, the comparable figure was 73% (Hasbi 2020, Table 2). The figures underestimate mobile phone use because it is not unusual for multiple individuals to own SIM cards but share a single phone (Hasbi 2020, p. 3). The rapid adoption of mobile phone technology is driven by the adoption of mobile payments. The adoption of this technology is rapidly transforming the *hawala* and money services industry. In Somalia, for example, mobile money is the primary access point to financial services (Elmi and Ngwenyama 2019, p. 119). Elmi, Mohamed and Ojelanki Ngwenyama, 2019, "The Role of Mobile Money in Somalia's Remittance System", in *HCI in Business, Government and Organizations*, edited by F.H. Nah and K. Siau, Basel: Springer Nature, pp. 119–36. In 2017, the World Bank estimated that 73% of the Somali population over the age of 16 used mobile money services (Elmi and Ngwenyama 2019, p. 119).

⁵⁴ APUNCAC arts. 30(iii), 70.

3.9. Front Men

Application of the proposed Rule would deter money laundering by deterring the participation of front men who enable money laundering. When money laundering occurs, including via trade-based money laundering and informal value transfer systems, it almost always involves front men at each end of the value transfer scheme. A 2018 FATF report titled “Professional Money Laundering” described four main types of money laundering schemes: (i) money transport and cash controller networks; (ii) money mule networks; (iii) digital money and virtual currency networks; and (iv) proxy networks (FATF 2018, p. 19). All four involved the use of front men to hide the identities of the true individuals controlling the transactions. In one instance, for example:

The money launderer instructed nominees to either (i) transfer funds back to the logistics company; or (ii) transfer funds to other business accounts, held by nominees located in Canada, China, Panama and the US. Funds were sent by wire transfer, bank draft or cheque. (FATF 2018, p. 31)

Another tactic involved opening and transferring money to and from bank accounts held in the names of individuals or offshore entities that served as front men (or front entities) for the true beneficial owners of the accounts (FATF 2018, p. 40). An April 2015 MONEYVAL “Typologies Report on Laundering the Proceeds of Organised Crime” found that the use of front men/straw men is one of the top six money laundering techniques used by organized crime groups (MONEYVAL 2015, p. 60). The report recited numerous case examples of money laundering involving front men.

When professional money launderers recruit attorneys, accountants, financial service professionals, Trust or Company Service Provider (TCSP) personnel, directors of shell companies, persons involved in TBML or IVTS, casino gamblers, money mules, students, relatives, and others to knowingly or unknowingly transact illicit funds in their own names or for the benefit of undisclosed beneficial owners, those recruits effectively serve as front men who (inadvertently or otherwise) serve to hide the identities of the true beneficial owners. When a person other than the true criminals controlling the transactions serves as a front man who effectively hides the identity of the criminals, that person enables the associated crime. There is a need to peel away this anonymity by forcing the front man to make a declaration regarding the identity of the true beneficial owner controlling the transaction. That declaration is either true or it is false. If it is false, a prosecutor gains the leverage needed to compel cooperation.

Unlike true beneficial owners, the front men receive directions, typically via text messages, from either the true beneficial owners or their agents. As described above, this means that front men are vulnerable to prosecution under the proposed Rule whenever prosecutors seize electronic devices, unlock them, and obtain access to these messages (see Sections 3.3 and 3.6–3.8). This gives prosecutors the leverage needed to obtain cooperation, obtain useful information identifying the criminals who orchestrate the activity, and unravel the criminal schemes. Once prosecutors have this leverage, they can unravel even the most complex, sophisticated, organized criminal networks. But the starting point is to establish the APUNCAC Rule and arm prosecutors with the legal tools needed to secure the cooperation of witnesses who have useful information.

While the Rule is simply a regulatory requirement, it would seek to deter the participation of the army of enablers required to move large amounts of illicit funds through these schemes. It would accomplish this by facilitating the prosecution of individuals who would otherwise have little to fear from prosecutors and currently act with impunity. It would provide a foundation for effective, efficient investigation, prosecution, and deterrence of the type of money laundering that facilitates organized crime.

A prosecutor who consistently traps front men could trigger a domino effect, whereby cooperation by a front man triggers successive cooperation agreements with each person in the chain of individuals directing the front man, until the person orchestrating the entire

criminal scheme is identified. The efficiency of this investigative technique would be expected to break down the stoutest criminal organization.

3.10. Money Mules

A money mule is a person who knowingly or otherwise allows his or her bank account, e-wallet, debit card, or stored value card to be used to launder illicit funds (Raza et al. 2020). A money mule is a type of front man whose identity is utilized by criminals to hide the identity of the true beneficial owner controlling financial transactions performed in the name of the money mule. Money mules are critical to the operation of large-scale professional money laundering schemes and organized crime.

Money mules may be teenagers, college students, new migrants, small business owners, elderly individuals, retirees, job seekers, or individuals seeking a romantic relationship (Raza et al. 2020). They may be recruited through personal contacts via chat rooms, social media, schools, soccer fields, employment ads, job boards, online job scams, email solicitation, or online romance schemes (Raza et al. 2020). They may be recruited for positions working for an international company as a “money transfer agent” or “payment agent” or may be asked to sell or lend their account password details for use by a friend or acquaintance (Raza et al. 2020). Money mules may or may not receive a commission for their services (Raza et al. 2020). Much communication occurs via phone-based text messages directing the money mules to transmit funds using their own bank accounts, e-wallets, debit cards, or stored value cards or to provide bank, e-wallet, debit card, or stored value card details to allow illicit funds to be transmitted and laundered.

Money mules may receive regular sums of cash to be deposited into their bank accounts. They may be directed to transfer the amounts to foreign bank accounts. They may receive a small commission for each transaction. A person who serves as a money mule may not know that the origin of the funds is illicit. Regardless, the APUNCAC Beneficial Owner Rule captures this activity by capturing “any person doing business, whether or not on a regular basis or as an organized business concern, who provides remittance services, makes or receives cash deposits or cash payments, or converts negotiable instruments or bearer instruments to cash as a financial service” (Section 2.3, above). The Rule requires such individuals to obtain and submit certification by the true beneficial owners of beneficial ownership whenever covered funds are sent or received in amounts exceeding USD 3000. A money mule who receives cash exceeding this amount would be required to obtain and submit a certification of beneficial ownership. Money mules who falsely self-certify beneficial ownership, including those who set electronic flags on their accounts that automatically self-certify beneficial ownership, would be vulnerable to prosecution if a prosecutor were to obtain, via seized electronic devices, incriminating text messages proving that the alleged beneficial owners were, in fact, serving as front men controlled by other individuals. Since prosecutors would not need to prove the illicit nature of the funds, the threat of prosecution would be genuine. Deterrence would, therefore, be relatively strong.

Contrary to popular belief, law enforcement has substantial capacity to access the content of encrypted messaging apps (Caesar 2023; Davis 2021; FBI 2021; NCA 2020; Pfefferkorn 2021). Regardless, prosecutors who catch money mules in illegal schemes can pressure them into cooperation agreements where they agree to cooperate in exchange for probationary sentences. This implies that money mules are a weak link vulnerable to prosecutorial pressure. Once they name the criminals who control them, prosecutors can utilize the APUNCAC Rule to threaten the named individuals with prosecution, obtain cooperation agreements, and obtain witness testimony regarding the criminal schemes and the individuals who control the schemes.

All money mules, including those who choose to sell their bank password details along with electronic flags falsely certifying beneficial ownership of covered transacted funds, would be vulnerable to prosecution and vulnerable to pressure to cooperate with prosecutors, reveal details about the criminals controlling the transactions, and testify against the criminals. Those criminals, in turn, would become vulnerable to prosecution

and vulnerable to pressure to cooperate with prosecutors, reveal details about the criminal masterminds controlling the operations, and testify against the criminal masterminds. In this way, the proposed Rule would provide a legal tool for prosecutors to unravel even the most complex organized criminal schemes. The proposed Rule would provide a tool for gaining the cooperation of insiders within criminal networks who have intimate knowledge of individual responsibilities and operational details, can testify regarding those responsibilities and details, and thereby secure the conviction of criminal masterminds controlling organized criminal schemes.

3.11. Bank Clerks

The MONEYVAL Report (2015) concluded that organized crime has infiltrated financial institutions and poses a serious threat, via bribery and corruption of financial institution personnel, to the integrity of the international financial system and anti-money laundering regime (MONEYVAL 2015, pp. 54–56). Organized crime groups (OCGs) utilize financial institution officers to tipoff the OCGs whenever authorities request data relating to transactions involving OCG-related companies, selectively abstain from checks and inspections in certain areas, not generate suspicious transaction reports (STRs), produce false documentation, forge documents, enter fictitious data, aid and abet the use of nominee beneficial owners to conceal beneficial ownership of illicit funds, misappropriate and embezzle funds, abuse their official powers, and knowingly participate in money laundering schemes (MONEYVAL 2015, pp. 54–56). In some cases, bank clerks (including, for example, a manager of a branch office and member of the bank board) were themselves members of an OCG (MONEYVAL 2015, p. 55). This implies that financial institution personnel, including bank clerks, who participate in these schemes would be vulnerable to prosecutorial pressure to enter into plea agreements and agreements to cooperate with prosecutors if and when they are caught.

The proposed APUNCAC Beneficial Owner Rule could not be avoided by financial institution personnel involved in schemes to hide beneficial ownership and launder illicit funds. If they become involved in schemes to violate the Rule, they would become vulnerable to prosecutorial pressure to cooperate and provide the information and testimony needed to pressure and gain the cooperation of insiders within the criminal networks who have intimate knowledge of individual responsibilities and operational details and can testify regarding those responsibilities and details, thereby securing the conviction of criminal masterminds controlling organized the criminal schemes.

3.12. Cooperation Agreements

Prosecution of organized crime has become a top policy priority (Fyfe and Sheptycki 2006, p. 319). To fight organized crime, an increasing number of countries have introduced legislation and policies to facilitate witness cooperation (Fyfe and Sheptycki 2006, p. 320). Testimony obtained from cooperating or ‘crown witnesses’ is now the central approach in the investigation and prosecution of organized crime” (Fyfe and Sheptycki 2006, p. 320).

Prosecutors in both the U.S. and Italy have achieved success in prosecuting mafia figures, relying heavily on the application of leniency programs that encourage witness cooperation (Jamieson 2000; Reuters 2021; Scotti 2002). Prosecutors have achieved success in obtaining witness cooperation despite the threat of retaliation. The fact that so many mafia cases have been successfully prosecuted with the assistance of cooperating figures suggests that leniency programs can be successful despite the risk of retaliation.

A review of international trends in the facilitation of witness cooperation in organized crime cases concluded: “Evidence provided by witnesses is vital to the effective investigation of crime. It helps to identify and build a case against the accused. Therefore, facilitating witness co-operation is a key objective of all criminal justice systems” (Fyfe and Sheptycki 2006, p. 349).

The proposed APUNCAC Rule seeks to open a flood of witness cooperation. This approach is validated by the success in prosecuting mafia figures. The Rule would provide

the leverage needed by prosecutors to negotiate formal or informal cooperation agreements with insiders who have intimate operational knowledge of criminal schemes and the criminals who orchestrate those schemes. Cooperation agreements are key to this strategy.

Cooperation agreements are enabled by legal systems that permit prosecutors and defendants to negotiate plea bargains where a defendant agrees to plead guilty to reduced charges. Legal provisions that permit plea bargains provide incentives to cooperate. Plea bargains facilitate either formal or informal cooperation agreements with defendants to tackle corruption and organized crime (see [Langer 2021](#), p. 382). These mechanisms permit negotiations in which the defendant may receive a reduction in sentencing in exchange for providing information or testimony against accomplices or other people involved in the commission of crimes (see [Langer 2021](#), p. 394).

Multiple international instruments require that states parties take measures, in accordance with their fundamental legal principles, to encourage the cooperation of witnesses with law enforcement authorities. These instruments include UNTOC (Article 26) and the United Nations Convention against Corruption (UNCAC, Article 37), which govern the behavior of all States Parties. Member States of the EU are, in addition, governed by the EU Council Resolution of 20 December 1996 on individuals who cooperate with the judicial process in the fight against international organized crime, and EU Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organized crime (Article 4).

Almost all nations, including civil as well as common law jurisdictions, are States Parties to UNCAC, which endorses the use of both sentence reduction mechanisms and grants of immunity in corruption cases to induce the cooperation of participants in the crime.⁵⁵ Article 37(1) requires that states “take appropriate measures to encourage persons who participate or have participated” in corruption offenses “to supply information useful to competent authorities for investigative and evidentiary purposes”, and to provide other factual help ([UNODC 2006](#), pp. 121, 49). Article 37 then goes on to specifically urge states to enact measures permitting “mitigating punishment of an accused person” and/or the “granting of immunity from prosecution to a person”, if the person “provides substantial cooperation in the investigation or prosecution” of corruption crimes ([UNODC 2006](#), pp. 121, 49).⁵⁶

A comparative analysis of legal regimes in the Netherlands, Germany, Italy and Canada found that incentives to cooperate, involving reductions in sentences, are legitimate and necessary: “in each of the four jurisdictions under consideration, collaboration with justice is considered a legitimate and necessary instrument in the investigation and/or prosecution of (serious) crime” ([Crijns et al. 2017](#), p. 322). These incentives entail “the granting of benefits in exchange for testimony in the prosecution of others” ([Crijns et al. 2017](#), p. 324).

Judicial acceptance of the type of plea bargaining that facilitates cooperation agreements has expanded across common law and civil law legal systems, including many systems oriented toward Islamic law. Plea bargaining and related mechanisms have spread worldwide over the past five decades; adoption has accelerated over the past 30 years ([Langer 2021](#), p. 405). Plea bargaining, penal orders, and related trial-avoiding conviction mechanisms are judicially recognized by high courts in 60 nations ([Langer 2021](#), Table 1). Most common law legal systems permit plea bargaining. Plea bargaining is widely accepted in civil law jurisdictions. Acceptance among legal systems oriented toward Islamic law is expanding.

⁵⁵ United Nations Convention against Corruption, *opened for signature* 31 October 2003 2349 UNTS 41 (entered into force December 14, 2005) [hereinafter UNCAC]. Of 196 nations, 189 are States Parties to UNCAC.

⁵⁶ *Id.* arts. 37(2)–(3).

3.12.1. Common Law Legal Systems

Plea bargaining and cooperation agreements are almost universally accepted across common law legal systems, including the United States, the United Kingdom, the Commonwealth Caribbean countries, Cyprus, Malta, Australia, and India.

United States

The U.S. legal system is a common law federal system. In the U.S., an agreement to cooperate may be formalized into a written agreement where a prosecutor agrees to make a motion during the sentencing phase, stating that a defendant has provided substantial assistance in the investigation or prosecution of another person who has committed an offense, contingent on the degree of cooperation provided by the defendant. This type of agreement is effective in combatting organized crime because the testimony of witnesses can be used to prosecute criminals who may otherwise be difficult to prosecute. An American court noted:

Promises of immunity are important weapons in the fight against large-scale criminal enterprises; the government often snares big fish with information gained from little fish. In return, the little fish are granted immunity from prosecution based upon the information they provide to the government.⁵⁷

“Sometimes the fish are all one size and the one who receives immunity may be simply the one who first shows a convincing readiness to cooperate” (Hughes 1992, fn 3). Defendants have an incentive to negotiate an early cooperation agreement. Prosecutors may determine that a defendant who elects to go to trial is especially deserving of rigorous prosecution compared with a defendant who demonstrates an early desire to plead and cooperate (Hughes 1992, fn 3).

A defendant who agrees to cooperate assumes significant obligations:

The cooperator makes a set of promises and assumes potentially onerous and protracted obligations. These will at least include interviews and debriefings and may involve undercover action or observation and reporting back. The cooperator’s obligations will probably continue into more formal stages with grand jury and trial testimony and, perhaps, testimony at retrials years later. (Hughes 1992, p. 3)

Cooperators are under strong pressure to provide useful information and to testify truthfully and consistently, even in the absence of explicit guarantees of immunity:

[T]he witness will know that he has no chance to gain immunity or leniency unless the information that he initially furnishes appears weighty enough to aid in convicting a target. At an early stage he almost certainly will testify before a grand jury. If this testimony differs in any significant way from the information he gave the police and the prosecutor, he may lose immediately any expectation of leniency or immunity, since it logically follows that either the information tendered to the police or the grand jury testimony was false. Similarly, if his testimony at trial differs either from the information tendered or from his grand jury testimony, he risks losing the benefits of the bargain and also risks prosecution for perjury. The prosecution thus may bring the strongest pressures to bear without, in the cooperation agreement, explicitly trading leniency or immunity for trial results. (Hughes 1992, p. 39)

Cooperation agreements are typically written to ensure that a breach by the defendant will forfeit any immunity regarding statements that would otherwise be protected (Hughes 1992, p. 49). Defendants must tell the truth, and they must tell the whole truth. Otherwise, they could easily be prosecuted based upon any of their statements. “The cooperator usually trades away his Fifth Amendment rights against self-incrimination” (Hughes 1992, p. 53).

⁵⁷ United States v. Palumbo, 897 F.2d 245, 246 (7th Cir. 1990).

A defendant who cooperates, however, may achieve substantial benefits in sentencing:

A court may reduce a sentence below the [Sentencing] Guidelines' lower limit if the government makes a motion stating that the defendant has provided substantial assistance in the investigation or prosecution of another person who has committed an offense. (Hughes 1992, p. 44)

The magnitude of the benefit depends on the degree to which the defendant cooperated with the prosecutor:

The court has discretion to determine the appropriate reduction in these cases, and the Guidelines provide that, in so doing, the court should give "substantial weight" to the government's evaluation. The cooperator, therefore, will want a government promise to make a favorable sentencing motion included in the cooperation agreement. This promise also strengthens the prosecutor's hand since her assessment of the truthfulness and impact of the cooperator's testimony will determine both whether the government makes the sentencing reduction motion at all and how favorable that motion will be. (Hughes 1992, p. 44)

For these reasons, cooperation agreements are powerful tools for obtaining useful information from insiders who are privy to damning details that can be utilized to prosecute individuals who orchestrate even the most complex, difficult to penetrate criminal schemes. Jurisdictions that do not currently utilize cooperation agreements could incorporate this type of agreement into their domestic legal regimes, with all the safeguards as the American system.

United Kingdom

England, Wales, and Northern Ireland operate common law legal systems. Scots law is a hybrid system that mixes elements of common law and civil law. In the UK, a defendant can offer a written guilty plea to a lesser offense with the same (or closely similar) facts as the offense charged, which has to be accepted by the court to take effect (Attorney General's Office 2012). The Serious Organised Crime and Police Act 2005 offers the option for a defendant to assist the prosecution and/or police by providing information to secure convictions of the principal offenders in return for immunity from prosecution (Section 71), a restricted use undertaking (a version of immunity) (Section 72) or a reduced sentence (Section 73).⁵⁸ Sentences may be reduced if an offender cooperates with an investigation pursuant to a written agreement with a prosecutor (Sentencing Council 2023).⁵⁹ In sum, UK law provides that a cooperating witness may exchange information and testimony for a reduced sentence or immunity from prosecution.

Commonwealth Caribbean Jurisdictions

Jurisdictions included in the term Commonwealth Caribbean are Anguilla, Antigua and Barbuda, the Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Dominica, Grenada, Guyana, Jamaica, Montserrat, St. Kitts and Nevis, St. Lucia, St. Vincent and The Grenadines, Trinidad and Tobago, and Turks and Caicos. Except for St. Lucia, the legal system of the English-speaking Caribbean countries is based on the common law system.

Commonwealth Caribbean jurisdictions permit plea bargaining, where a defendant may, by statute or common law, negotiate with a prosecutor to plead guilty to a lesser offense, subject to court approval (see Seetahal and Ramgoolam 2019, p. 98). A prosecutor may accept or reject this plea (Seetahal and Ramgoolam 2019, p. 98). A prosecutor may agree in advance to accept a plea of guilty to a lesser offense (Seetahal and Ramgoolam 2019, p. 101). In 1999, Trinidad and Tobago enacted a system of plea bargaining by means of the

⁵⁸ Serious Organised Crime and Police Act 2005 §§ 71–73. These sections do not apply to Scotland. See Serious Organised Crime and Police Act 2005, <https://www.legislation.gov.uk/ukpga/2005/15/section/179>, accessed 22 September 2023.

⁵⁹ Sentencing Act 2020 § 74(1)(c).

Criminal Procedure (Plea Discussion and Plea Agreement) Act No. 11 of 1999, Chapter 13:07 (Seetahal and Ramgoolam 2019, p. 101). In December 2008, Guyana enacted a system of plea bargaining by virtue of Act 18 of 2008 (Seetahal and Ramgoolam 2019, p. 101). Jamaica enacted a system of plea bargaining via the Jamaica Criminal Justice (Plea Negotiations and Agreement) Act of 2005 (Seetahal and Ramgoolam 2019, p. 101). A prosecutor and the accused or his attorney may engage in plea discussions (Seetahal and Ramgoolam 2019, p. 101). Any subsequent agreement is subject to court approval (Seetahal and Ramgoolam 2019, p. 101).

In sum, Commonwealth Caribbean law permits a cooperating witness to exchange information and testimony for a reduced sentence or immunity from prosecution. The significance is that this type of cooperation agreement is permitted in high-risk money laundering jurisdictions, including the Bahamas, the British Virgin Islands, and the Cayman Islands.

Cyprus

Cyprus has adopted a common law legal system. Cyprus permits plea negotiations and bargaining between prosecutors and defendants (Kyprianou 2006, pp. 259–60). A prosecutor may decline to prosecute some co-defendants in exchange for their testimony against others (see Kyprianou 2006, p. 258). For example, in a case involving a series of frauds and abuse of power by a senior public servant, Cypriot prosecutors chose not to prosecute his accomplices because this was the only way to convince them to testify against him (Kyprianou 2006, p. 258). In sum, Cypriot law permits a cooperating witness to exchange information and testimony for a reduced sentence or immunity from prosecution. The significance is that this type of cooperation agreement is permitted in Cyprus, a high-risk money laundering jurisdiction.

Malta

Malta has adopted a mixed system of civil and common law. Article 453A of Malta's Criminal Code established a system of plea bargaining where a defendant may negotiate an agreement with the Attorney General to plead guilty and to request that a court apply "a combination of sanctions or measures, of the kind and quantity agreed between them".⁶⁰ Significantly, "courts treat plea bargains as contracts between prosecutors and defendants" (Said 2022). Agreements are subject to court approval.⁶¹ An agreement may involve a suspended sentence.⁶² The system of plea bargaining is widely used. "Prosecutors often offer favorable plea bargains to defendants who agree to testify for the State in cases against other defendants" (Said 2022). In sum, Maltese law permits a cooperating witness to exchange information and testimony for a reduced sentence or immunity from prosecution. The significance is that this type of cooperation agreement is permitted in Malta, a high-risk money laundering jurisdiction.

Australia

The Australian legal system is based on the British common law system. In Australia, a defendant may agree to plead guilty to reduced charges in exchange for information or testimony that assists in the investigation or prosecution of others (Director of Public Prosecutions South Australia 2014, p. 10). Charges may be reduced if "the accused is willing to co-operate in the investigation or prosecution of others, or the extent to which the accused has done so" (Director of Public Prosecutions South Australia 2014, p. 10). "[N]egotiations may result in the accused pleading guilty to fewer than all of the charges he or she is facing, or to a lesser charge or charges, with the remaining charges either not being proceeded with or taken into account without proceeding to conviction" (Director of

⁶⁰ MALT. CRIM. CODE art. 453A(1).

⁶¹ *Id.* art. 453A(2).

⁶² *Id.* art. 453A(3).

[Public Prosecutions South Australia 2014](#), p. 10). In sum, Australian law provides that a cooperating witness may exchange information and testimony for reduced charges.

India

The Indian legal system is based on the British common law system. In 2005, India enacted a system of plea bargaining that allows defendants to negotiate with a prosecutor and enter into a written agreement to plead guilty to a lesser charge ([Pathak 2015](#)).⁶³ Excluded are offenses that affect “the socio-economic condition of the country or [have] been committed against a woman, or a child below the age of fourteen years”.⁶⁴ Socioeconomic offenses are covered by statutes regarding dowry and protection of women from domestic violence. “[I]n a case instituted on a police report, the Court shall issue notice to the Public Prosecutor, the police officer who has investigated the case, the accused and the victim of the case to participate in the meeting to work out a satisfactory disposition of the case”.⁶⁵ Upon reaching an agreement, a court may reduce or suspend a sentence.⁶⁶ In principle, the system permits a cooperating witness to exchange information and testimony against accomplices for reduced charges.

3.12.2. European Civil Law Systems

The use of formal or informal cooperation agreements is increasingly being adopted in civil as well as common law jurisdictions (see [Wagner and Jacobs 2008](#), p. 229). In November 2007, the European Commission acknowledged that “nearly all [EU Member States] provide the possibility for the court judge to give a lighter punishment to offenders who help the police/judicial authorities to clarify their or other crimes” ([European Commission 2007](#)). The type of plea bargaining that facilitates cooperation agreements is currently regulated and accepted in 27 European civil law countries ([Bicek 2022](#)).

The use of crown witnesses “has developed into an essential instrument in the fight against serious crime” ([Tak 1997](#), p. 19). In Europe, several jurisdictions rely on the use of crown witnesses to tackle organized crime. In Italy, for example, crown witnesses (or ‘*pentiti*’) benefit from reward regulations (or ‘*premi*’), where a judge may decide not to sentence or to impose a less severe sentence on these informants ([Fyfe and Sheptycki 2005](#), p. iv; [2006](#), p. 336, Table 2). To ensure the truthfulness of statements, a review procedure exists that allows the sentence to be raised if a crown witness had made false statements ([Fyfe and Sheptycki 2005](#), p. iv; [2006](#), p. 336, Table 2). The Mafia *pentiti* crown witness regulation has been “a great success” ([Tak 1997](#), p. 22). “The number of ‘singing’ Mafiosi has increased explosively over the past years” ([Tak 1997](#), p. 22). Jurisdictions that recognize and permit cooperation agreements include Germany, Italy, Northern Ireland, and Spain, as well as the United States ([Fyfe and Sheptycki 2005](#), Table 3.1; [2006](#), p. 336, Table 2). The use of crown witnesses is crucial in the fight against organized crime (see [Tak 1997](#), p. 19).

Sentence reduction for cooperating witnesses was endorsed by the member states of the European Union via the 2008 Framework decision of the European Council:

Each Member State may take the necessary measures to ensure that the penalties referred to in Article 3 may be reduced or that the offender may be exempted from penalties if he, for example: (a) renounces criminal activity; and (b) provides the administrative or judicial authorities with information which they would not otherwise have been able to obtain, helping them to: (i) prevent, end or mitigate the effects of the offence; (ii) identify or bring to justice the other offenders.⁶⁷

In December 2014, the 46 member states of the Council of Europe, including France, Germany, Italy, and Spain, published a “white paper” on the topic of transnational or-

⁶³ CODE CRIM. PROC. §§ 265A–265H.

⁶⁴ *Id.* § 265A.

⁶⁵ *Id.* § 265C(a).

⁶⁶ *Id.* § 265E.

⁶⁷ Council Framework Decision No. 2008/841/JHA art. 4, 2008 O.J. L 300/42.

ganized crime (Council of Europe 2014). The document noted that “the co-operation of insiders is crucial in investigating and combating [transnational organized crime]” (Council of Europe 2014, p. 30).

States parties are encouraged in particular to provide for the possibility of mitigating punishment or granting immunity from prosecution to persons providing substantial co-operation in the investigation or prosecution of a related offence, not only in a domestic, but also in a transnational context. (Council of Europe 2014, p. 31)

The document urged states parties to consider “various forms of plea bargaining, pre-judicial co-operation agreements and summary prosecutions, as already used or being developed by a number of Council of Europe member states (e.g., Azerbaijan, Estonia, Switzerland, the UK)” (Council of Europe 2014, pp. 31–32). The document urged states parties to consider entering into agreements concerning the potential provision of preferential treatment by the competent authorities of one state to a cooperating person located in another (Council of Europe 2014, p. 32). The document recommended analysis of “incentives to encourage the co-operation of collaborators” including “forms of plea bargaining and pre-judicial co-operation agreements that may result in a mitigated punishment” (Council of Europe 2014, p. 41). “As a further step”, the document suggested “a recommendation or even binding provisions... that would stress the importance of effective, harmonised measures in this field, and urge their adoption by member states” (Council of Europe 2014, p. 32).

This recommendation aligns with the existing practice across Europe of using criminal informants to prosecute cases of organized and serious crime (see Fyfe and Sheptycki 2005, p. 18). In many countries in Western Europe, police “have developed a considerable capacity to identify and recruit criminal informants in the illicit or underground economies that feed organized crime” (Fyfe and Sheptycki 2005, p. 18). “Most states parties have measures of a generic nature in place (usually to be found in their criminal codes), permitting collaboration to be considered as a circumstance mitigating criminal liability and taken into account by the court during sentencing” (Council of Europe 2014, p. 31).

France

The French legal system is a prototypical European civil law system. In 2004, France implemented a plea bargaining procedure (*Comparution sur Reconnaissance Préalable de Culpabilité* or CRPC), which involves a pre-trial guilty plea by an offender.⁶⁸ The procedure “requires both defense and prosecution to engage in a pretrial agreement, and judge and prosecutor to share power in case disposition” (Hodgson 2020, p. 20). In practice, the sentence is negotiated directly between the public prosecutor and the accused (Hodgson 2012, p. 127). “The prosecutor discusses the proposal directly with the accused; the defense lawyer is asked to agree the sentence; and the judge is required to confirm or reject that sentence in court” (Hodgson 2020, p. 20). The procedure was extended in 2011 to include most offenses, including the crime of corruption, punishable by imprisonment of up to ten years (*délits*). In March 2019, France amended the procedure to allow the public prosecutor to propose a prison sentence of up to three years (Ministry of Justice 2019, p. 7). This effectively extended the procedure to serious crimes that had previously been excluded.⁶⁹

The public prosecutor may, before proposing a sentence, inform the defendant of the proposed sentence (Ministry of Justice 2019, p. 8). These provisions allow a preliminary discussion between the prosecution and the defendant or his lawyer before the prosecutor, in light of any comments by the defendant or his lawyer, formulates a proposal for a final sentence, thereby encouraging a defendant to accept the proposed sentence (Ministry of

⁶⁸ C. PR. PÉN. §§ 495-7, 495-8.

⁶⁹ The CRPC procedure may be applied to economic crimes punishable by imprisonment of up to ten years. For this type of serious crime, a trial judge may be reluctant to accept a sentence recommendation of one year imprisonment but may be amenable to a sentence recommendation of three years imprisonment. The change in law effectively extends the applicability of the CRPC procedure to a greater range of crimes.

Justice 2019, p. 8). The public prosecutor was authorized to propose a prison sentence that would revoke a previous suspended sentence (Ministry of Justice 2019, p. 8). These actions by the public prosecutor are optional (Ministry of Justice 2019, p. 9). The public prosecutor will assess, on a case-by-case basis, the advisability of recourse to these options (Ministry of Justice 2019, p. 9). The public prosecutor may intervene at the investigation stage (Ministry of Justice 2019, p. 9).

These provisions create opportunities and incentives for defendants to cooperate with prosecutors and provide useful information during the investigation stage in exchange for leniency in recommended sentences. “French public prosecutors have great influence over the punishment handed down by the courts. Not only do they decide whether to prosecute or not and on what charge, but they also recommend a sentence at trial” (Hodgson and Soubise 2016, p. 228). “Almost half of the cases (45 percent) were settled by public prosecutors through alternatives to prosecution” (Hodgson and Soubise 2016, p. 228).

French law permits the public prosecutor to engage in a preliminary discussion with a defendant, weigh the value of information provided by the defendant, arrive at a pretrial sentencing agreement, and then recommend a fine, a suspended sentence, or a sentence that is a fraction of the maximum sentence (Ministry of Justice 2019, pp. 7–9). This procedure encourages defendants to cooperate with the public prosecutor. Cooperative defendants are likely to be rewarded with reduced sentences.

French law explicitly immunizes a participant in a conspiracy “established with a view to the preparation” of a crime punishable by five or more years imprisonment “if, before any prosecution is instituted, he discloses the existence of the group or conspiracy to the competent authorities and enables the other participants to be identified”.⁷⁰ In sum, French law provides that a cooperating witness may exchange information and testimony against accomplices for immunity from prosecution.

3.12.3. Non-European Civil Law Systems

The adoption of plea bargaining and the use of cooperation agreements in civil law legal systems is now widespread. Non-European civil law jurisdictions that utilize plea bargaining and cooperation agreements include Brazil, Mexico, Japan, China, Russia, and South Africa.

Brazil

Brazil has adopted a civil law legal system. In August 2013, Brazil enacted a system of plea bargaining that allows suspects and defendants to enter into written cooperation agreements (*colaboração premiada*) where information and testimony are exchanged for a reduction in sentencing.⁷¹ A judge may, at the request of the parties, grant judicial pardon to, or reduce by up to two-thirds or replace with a sentence of restrictive rights the custodial sentence of those who have cooperated effectively and voluntarily with an investigation and criminal prosecution leading to the identification of participants in a criminal organization and of criminal offenses committed by them (Library of Congress 2013). The Brazilian legal system explicitly permits plea bargains and cooperation agreements.

Mexico

Mexico has adopted a civil law legal system. In June 2016, Mexico implemented a package of legal reforms, including a system of plea bargaining (*juicio abreviado*) (see Shirk 2016, pp. 203–4). “A due process judge, or *juez de garantías*, will preside over the pre-trial phase (investigation, preliminary hearing, indictment, and plea-bargaining)” (Shirk 2016, p. 209). The due process judge is invested with the responsibility of ensuring due

⁷⁰ C. PÉN. arts. 450-1, 450-2 (trans. J. R. Spencer) (“Any person who has participated in the group or the conspiracy defined by article 450-1 is exempted from punishment if, before any prosecution is instituted, he discloses the existence of the group or conspiracy to the competent authorities and enables the other participants to be identified”).

⁷¹ Law 12,850/2013 art. 4 (Brazil, trans. Court of Justice of the Federal District and Territories—TJDFT).

process during the pre-trial phase (Shirk 2016, p. 209). The due process judge issues a final sentence in cases in which a defendant accepts a plea bargain (Shirk 2016, p. 211). A plea bargain involves an agreement where a defendant pleads guilty in exchange for a lesser sentence (Shirk 2016, p. 211). The plea-bargaining procedure permits a cooperating witness to exchange testimony against accomplices for a reduced charge or immunity from prosecution.

Japan

Japan has adopted a civil law legal system. Effective June 2018, Japan implemented a system of plea bargaining that allows suspects and defendants to enter into negotiations with prosecutors whereby evidence of others' criminal conduct can be provided in return for criminal charges being reduced or dropped (Nagashima Ohno & Tsunematsu 2020). The system covers financial crimes (Nagashima Ohno & Tsunematsu 2020). "[T]he public prosecutor may reach an agreement with the suspect or accused [to provide] necessary cooperation", e.g., testimony.⁷² In exchange, a prosecutor may reduce or drop charges.⁷³ In sum, Japanese law provides that a cooperating witness may exchange information and testimony against accomplices for immunity from prosecution. The Japanese legal system, traditionally least amenable to plea bargains and cooperation agreements, now permits such agreements.

China

China has adopted a civil law legal system. In 2018, China enacted a system of plea bargaining into Chinese Criminal Procedure Law (Shi 2021, p. 88). "All types of cases can be addressed through plea bargaining" (Shi 2021, p. 89). "In the first half of 2020, 82.2% of cases were resolved through plea bargaining" (Shi 2021, p. 89). Chinese prosecutors are granted a leading role. Prosecutors can dismiss charges (Shi 2021, p. 96). They "decide which cases are suitable for plea bargaining, which type of process can be applied, and give recommendations as to the sentencing, which judges shall in principle follow" (Shi 2021, p. 88). Courts accepted 92.1% of all sentencing recommendations (Zhou 2017). Prosecutors have comprehensive discretion regarding the contents of plea bargaining agreements with suspects (Liu 2020). In principle, the plea-bargaining procedure permits a cooperating witness to exchange testimony against accomplices for a reduced charge or immunity from prosecution.

Russia

Russia has adopted a civil law legal system. "In 2001, Russia introduced a type of plea bargaining, known as 'special procedure court hearings,' that is now widely used" and has transformed the Russian criminal justice system (Solomon 2012, p. 282). Defendants who admit guilt and opt for the special procedure receive leniency in sentencing (see Solomon 2012, p. 283). The upper third of the normal sentencing range is excluded (Solomon 2012, p. 283). This permits deal making in the form of explicit agreements about charges, sentences, or sentencing recommendations in exchange for cooperation (see Solomon 2012, p. 284). "In 2009, the government adopted another version of the special procedure to be used when a defendant agreed to cooperate with an investigation, for example to expose superiors in a drug ring" (Solomon 2012, p. 289).

Rather than eliminate the upper third of the sentencing range, the law allows the judge to assign a punishment below the legal limit for the crime, or a suspended sentence, or simply no punishment at all. Moreover, the provisions on cooperation agreements openly invite negotiations over the plea. (Solomon 2012, p. 289)

⁷² Keiji Soshoho (Code of Criminal Procedure), Law No. 131 of 1948 art. 350-2 (Japan, trans. Ministry of Justice) [hereinafter KEISOHO].

⁷³ *Id.* art. 350-2.

In sum, the plea bargain procedure permits a cooperating witness to exchange testimony against accomplices for a reduced charge or immunity from prosecution.

South Africa

South Africa has adopted a mixed legal system that combines Roman-Dutch civil law, English common law, customary law, and religious personal law. South Africa enacted a system of plea and sentence agreements that allows defendants to negotiate with a prosecutor and enter into a written agreement to plead guilty to a lesser charge, subject to court approval.⁷⁴ “Plea bargaining is explicitly allowed [by] the National Prosecuting Authority of South Africa” (Majozi 2019, p. 86). Prosecutors have wide discretion to negotiate with defendants regarding the content of an agreement (Majozi 2019, p. 63). A defendant may negotiate an agreement where information or testimony regarding accomplices is exchanged for sentence reduction or immunity (see Majozi 2019, p. 75). Agreements are enforceable, promoting cooperation: “[T]he plea agreement is actually [an] obligatory and enforceable arrangement” (Majozi 2019, p. 62). In sum, South Africa permits a cooperating witness to exchange testimony against accomplices for sentence reduction or immunity from prosecution.

3.12.4. Islamic Criminal Justice Systems

Islamic criminal justice systems impose unique principles and constraints compared to common and civil law systems. Unlike common and civil law systems, Islamic criminal law derives rules and principles from “the Qur’an, Hadith and other secondary sources of Islamic law” (Babaji and Danjuma 2015, p. 63). Plea bargaining is a concept that may be viewed, under Islamic law, as incompatible with specified offenses “within the rights of Allah”, involving rights protected by the Qu’ran, whose penalties are mandatory and non-negotiable (al-Alfi 1982, pp. 227–28; Babaji and Danjuma 2015, pp. 71–73). However, plea bargaining may be viewed as compatible with Islamic law to the extent that it is limited to “*ta’azir* offences”, including bribery, corruption, and financial crimes, that do not have prescribed punishments under Islamic law (al-Alfi 1982, p. 228; Babaji and Danjuma 2015, pp. 71–73; Ismail 2021). Under Islamic law, the punishment of *ta’azir* offenses is at the discretion of a judge and, therefore, may be negotiated (al-Alfi 1982, pp. 228–30; Babaji and Danjuma 2015, pp. 71–72; Ismail 2021). The application of plea bargaining to offenses that do not have prescribed punishment in Islamic law can be said to be legal as it does not contravene the rulings of Allah (Babaji and Danjuma 2015, pp. 71–73; Ismail 2021).

Under Islamic law, white-collar crimes, “cover[ing] governance matters, decision making, rules through rebuking the misuse of trust placed in public servants through acts such as accepting gifts, utter misappropriation or embezzlement of public funds, and undermining rules in exchange for bribes, on recommendation or due to family and tribal considerations (peddling/trafficking in influence)”, “are penalized by *ta’azir* that includes all crimes, as corruption, in which Sharie’a does not prescribe a specific penalty” (‘Arafa 2018, pp. 3–4). “The punishment is left to the discretionary power delegated to the *qadi* (judge)” (‘Arafa 2018, p. 4).

Since a violation of the APUNCAC Beneficial Owner Rule would be a white-collar crime involving a violation of anti-money laundering regulations, it would be classified as a *ta’azir* offense, penalized at the discretion of a court by a maximum of five years imprisonment. The penalty for such an offense is, under Islamic law, discretionary and thus negotiable. Regardless of existing criminal procedure codes in Islamic countries, there is nothing in Islamic law that is fundamentally inconsistent with the application of plea bargaining and cooperation agreements involving plea bargains to violations of the proposed APUNCAC Beneficial Owner Rule. This implies the possibility that criminal procedure codes in Islamic countries that do not permit plea bargaining could potentially

⁷⁴ Criminal Procedure Act 1977 § 105A (South Africa).

be adapted to accommodate plea bargains and cooperation agreements regarding violations of the APUNCAC Rule and other *ta'azir* offenses.

In practice, national criminal justice systems in Islamic countries exist on a continuum where principles of Islamic law are combined, to a varying degree, with elements of civil and common law systems. In the strictest Islamic countries, such as the Persian Gulf, North African, and Central Asian states, plea bargaining is currently not permitted. However, notwithstanding Islamic legal strictures, Islamic countries, including Pakistan, Indonesia, Malaysia, Nigeria, Ethiopia, and Turkey, permit (or will soon permit) plea bargaining. In addition, plea bargaining is practiced informally in Iran. Plea bargaining has been enabled through legal reforms that have accelerated over the past decade. In sum, while plea bargaining is not permitted in many Islamic states, the adoption of the practice of plea bargaining has accelerated and has gained acceptance across numerous Islamic jurisdictions with large Muslim populations.

Pakistan

The Constitution of Pakistan states, as a matter of law, that Pakistani Muslims “shall” be enabled “to order their lives in accordance with the fundamental principles and basic concepts of Islam”.⁷⁵ The Pakistani legal system applies the principles of Islamic law in a system derived from English common law. Notwithstanding Islamic legal strictures, the National Accountability Bureau Ordinance of 1999 enacted plea bargaining in corruption cases (Babaji and Danjuma 2015, p. 72).⁷⁶ In 2021, Pakistan’s Ministry of Law drafted an amendment that would insert a new chapter regarding plea bargaining into the Code of Criminal Procedure (CrPC) (Malik 2021).⁷⁷ A plea bargain would involve “an agreement between the prosecutor and the defendant, wherein the defendant agrees to plead guilty in return for concessions from the prosecutor” (Iqbal 2022). Excluded are offenses that impact the socio-economic state of the country or when an offense has been committed against a woman or a child below the age of 18 (Iqbal 2022). In principle, the plea-bargaining procedure would permit a cooperating witness to exchange testimony against accomplices for a reduced charge or immunity from prosecution.

Indonesia

The Indonesian legal system combines secular and Islamic law in a civil law system based on the Roman-Dutch model. Article 24 of the Constitution established four parallel systems of courts, each with its own competencies (Cammack and Feener 2012, p. 20). The Islamic courts comprise one of these systems (Cammack and Feener 2012, p. 20). Furthermore, “In 1999, the province of Aceh was granted special autonomy status that included the authority to enforce Islamic law in areas beyond the established jurisdictions of Shari’a courts in the rest of the country” (Cammack and Feener 2012, p. 13).

Notwithstanding Islamic legal strictures, Indonesia drafted a new code of criminal procedure (RKUHAP) that seeks to enact a system of plea bargaining.⁷⁸ Article 199 will permit a defendant to plead guilty in exchange for a reduced sentence that may not exceed 2/3 of the maximum sentence for the crime charged (see Tristante 2018, pp. 416, 18–19).⁷⁹ Article 200 will enact a crown witness system that permits a witness to exchange testimony against accomplices for immunity from prosecution:

One of the suspects or defendants whose role is the lightest can be used as a witness in the same case and can be acquitted from criminal prosecution, if

⁷⁵ PAK. CONST. art. 31(1).

⁷⁶ National Accountability Bureau Ordinance 1999 § 25.

⁷⁷ PAK. CODE CRIM. PROC. ch. XXIB (Proposed Official Draft 2021).

⁷⁸ INDON. CODE CRIM. PROC. (draft) [hereinafter RKUHAP].

⁷⁹ *Id.* art. 199.

the witness helps reveal the involvement of other suspects who deserve to be punished for the said crime.⁸⁰

The public prosecutor determines the [the status of a] suspect or defendant as a crown witness.⁸¹

In sum, Indonesia will implement a system of plea bargaining and cooperation agreements that permits a cooperating witness to exchange information and testimony against accomplices for sentence reduction or immunity from prosecution.

Malaysia

Section 3(1) of the Constitution of Malaysia states that Islam is the religion of the Federation of Malaysia. Malaysia combines an Islamic legal system that operates in parallel with a common law legal system. In 2010, Malaysia enacted Section 172C of the Criminal Procedure Code, which allows plea bargaining to be exercised between the accused and the prosecutor regarding a charge or sentence ([Ab Aziz et al. 2017](#), p. 308; [Babaji and Danjuma 2015](#), p. 72).⁸² Notwithstanding Islamic legal strictures, all types of offenses are eligible for plea bargaining, including offenses that might otherwise be excluded under Islamic law (see [Babaji and Danjuma 2015](#), p. 72). The parties negotiate a written agreement regarding the charge or the sentence, subject to court approval (see [Ab Aziz et al. 2017](#), p. 308). The sentence may not exceed half the maximum sentence (see [Ab Aziz et al. 2017](#), p. 308).⁸³ In principle, the plea bargain procedure would permit a cooperating witness to exchange testimony against accomplices for a reduced charge or immunity from prosecution.

Nigeria

Nigeria, the most populous country in Africa, has adopted a mixed legal system comprising English common law, sharia, and customary law. Notwithstanding Islamic legal strictures, Section 494 of the Administration of Criminal Justice Act 2015 authorizes plea bargains, defined as a “process in criminal proceedings where the defendant and the prosecution work out a mutually acceptable agreement as to a lesser offense than what was actually charged in the complaint or information and in conformity with other conditions imposed by the prosecution, in return for a lighter sentence”, subject to court approval ([Egbegi 2020](#), p. 5).⁸⁴ Section 75 of the Administration of Criminal Justice Law of Lagos State 2007 authorizes the Attorney General to consider and accept a plea bargain “from a person charged with any offence, where the Attorney-General is of the view that the acceptance of such plea bargain is in the public interest, the interest of justice and the need to prevent the abuse of legal process”.⁸⁵ In principle, Nigeria permits a cooperating witness to exchange testimony against accomplices for a reduced charge or immunity from prosecution when an agreement is in the public interest.

Ethiopia

The Ethiopian legal system combines secular and Islamic law in a civil law system, with procedural laws based on common law. Notwithstanding Islamic legal strictures, Ethiopia’s Ministry of Justice published a report in February 2003 titled “Federal Democratic Republic of Ethiopia Criminal Justice Policy”, that recommended amendment of Ethiopian laws to establish a plea bargaining procedure where a defendant would agree with a prosecutor to plead guilty to a reduced charge or set of charges, involving a sentence reduction ([Ministry of Justice 2003](#), pp. 36–37). In 2013, the Ministry of Justice published a draft Criminal

⁸⁰ *Id.* art. 200(1).

⁸¹ *Id.* art. 200(3).

⁸² Criminal Procedure Code (Amendment) Act 2012 of Malaysia (codified at MALAY. CRIM. PROC. CODE § 172C).

⁸³ MALAY. CODE CRIM. PROC. § 172(D)(1)(c)(ii).

⁸⁴ Administration of Criminal Justice Act 2015 (Nigeria) § 494.

⁸⁵ Administration of Criminal Justice Law of Lagos State 2007 § 75.

Procedure Code incorporating a broad system of plea bargaining vested in the public prosecutor (Meheretu 2016, p. 412; Republic of Ethiopia 2013).⁸⁶ The Code gives broad discretion to a prosecutor regarding concessions (Meheretu 2016, p. 412). An evaluative analysis characterized Ethiopia's planned plea bargaining system as an "unrestrained model with minor modifications" (Meheretu 2016, p. 413). Preparations to implement the Code advanced with the issuance of Proclamation No. 691/2010 and Proclamation No. 943/2016, entrusting the Attorney General with the power to plea bargain (Negash 2018, p. 348). Thus, the implementation of the planned system of plea bargaining in the Ethiopian justice system is well-advanced.

A quasi-plea bargaining procedure involving cooperation agreements where suspects receive lenient treatment or immunity in exchange for cooperating in the prosecution of others is already recognized under the Anti-Corruption,⁸⁷ Anti-terrorism,⁸⁸ and Witness and Whistle-blower's Protection Proclamations⁸⁹ (Negash 2018, p. 348). In sum, Ethiopia permits cooperation agreements where defendants receive lenient treatment or immunity in exchange for cooperation and is in the process of implementing a broad model of plea bargaining that would facilitate cooperation agreements.

Iran

The Iranian criminal justice system is a civil law system. The Constitution of the Islamic Republic of Iran states that the form of government is an Islamic Republic and operates in conformity with Qur'anic law and principles: "Legislation setting forth regulations for the administration of society will revolve around the Qur'an and the Sunnah".⁹⁰ Article 4 states:

All civil, penal, financial, economic, administrative, cultural, military, political, and other laws and regulations must be based on Islamic criteria. This principle applies absolutely and generally to all articles of the Constitution as well as to all other laws and regulations.⁹¹

Notwithstanding Islamic legal strictures, and despite the lack of a provision in the Iranian code of criminal procedure, plea bargaining occurs informally (Kianersi et al. 2022, p. 117). Three Persian legal scholars recommended the insertion of a provision into Iranian law that would formally recognize plea bargaining, defined as a formal agreement negotiated between a prosecutor and the accused where the accused would admit to a crime in exchange for a reduction in the legal penalty, for *ta'azir* offenses (Kianersi et al. 2022, pp. 116–17). In sum, plea bargaining occurs informally in Iran, and there is support from legal scholars to formalize the procedure. The Iranian legal system is not inconsistent with the use of agreements where a defendant would receive lenient treatment in exchange for cooperation, including testimony against accomplices, regarding *ta'azir* offenses, such as bribery, corruption, and financial crimes.

Turkey

While Turkey has adopted a civil law legal system replacing Ottoman law and Sharia courts, 99.8 percent of the population identifies as Muslim, with strong Islamic influences on Turkish society (see CIA 2023). Notwithstanding Islamic legal strictures, Turkey enacted a simple trial procedure in 2019, applicable to crimes punishable by a judicial fine and/or imprisonment of two years or less, where a court may render a decision without holding a hearing, taking account of the public prosecutor's opinion, where the penalty would

⁸⁶ ETH. CODE CRIM. PROC. (draft) arts. 219, 221, 230 [hereinafter FDRE Draft Code].

⁸⁷ The Federal Anti-Corruption Special Procedure and Rules of Evidence (Amendment) Proclamation, Proclamation No. 239/2001 art. 43(1).

⁸⁸ The Anti-Terrorism Proclamation No. 652/2009 art. 33.

⁸⁹ Protection of Witnesses and Whistle-blowers of Criminal Offences Proclamation No. 699/2010 art. 3.

⁹⁰ IRAN CONST. art. 1, preamble.

⁹¹ *Id.* art. 4.

be reduced by a quarter (Sogut 2019). The system permits a cooperating witness to offer information and testimony against accomplices in exchange for reduced charges. Article 221 of the Turkish Penal Code (TCK), called the “active repentance” law, reduces or nullifies the prison sentences of defendants who provide information, testify against accomplices, or otherwise cooperate with investigators (Bozkurt 2022).⁹² In sum, Turkey permits a cooperating witness to exchange testimony against accomplices for sentence reduction or immunity from prosecution.

3.12.5. Cooperation Agreements—Summary

In both civil and common law jurisdictions, including a growing number of jurisdictions influenced by Islamic law, as well as communist systems, formal or informal cooperation agreements are increasingly being adopted as a legal tool because they are effective in prosecuting and combating corruption and organized crime.

The information provided by an immunized witness or cooperating defendant can be a tremendous evidence-gathering tool, both in strengthening the government’s case against known targets, or in initiating new investigations. They may be asked to produce documents, lead investigators to other evidence, and if it is still feasible, they may be directed to make recorded telephone calls or to meet with other targets of the investigation and record those meetings. The cooperation agreement mechanism not only yields valuable evidence, but gives prosecutors critical leverage within the criminal network. Since a participant in a corrupt relationship is usually in a position to provide highly incriminating evidence against other participants, the knowledge that an “insider” is cooperating with the prosecution is often enough on its own to convince other defendants to plead guilty. Because the first person to cooperate in an investigation often provides the most valuable information to investigators, that defendant often gets the largest reduction in sentence. Thus, once an investigation becomes overt and the scope of the investigation becomes known, or after indictment, lesser targets or defendants often “race” to be the first one in the case to cooperate, cracking the corrupt network wide open. (Wagner and Jacobs 2008, p. 229)

The international adoption of procedures that encourage defendants to cooperate with prosecutors in exchange for leniency in recommended sentences implies that implementation of the APUNCAC Rule could be combined with the use of cooperation agreements to secure the cooperation of bank clerks, front men, and other enablers of money laundering, unravel criminal schemes that involve money laundering, and prosecute the criminals who orchestrate these schemes.

Adoption of laws permitting cooperation agreements across civil law jurisdictions, including France, Germany, Italy, Spain, Switzerland, the Netherlands, Japan, Brazil, Mexico, China, Russia, South Africa, Nigeria, Turkey, Malaysia, Pakistan, Indonesia, and Ethiopia suggests that such agreements are compatible with civil, as well as common, law legal systems, jurisdictions influenced by Islamic law, and communist systems.

3.12.6. Viability of Cooperation Agreements

The viability of cooperation agreements as a strategy for securing the cooperation of bank clerks and front men is supported (a) by the preceding review of legal systems in Canada, the U.S., UK, Commonwealth Caribbean Countries, Cyprus, Malta, Australia, India, European civil law jurisdictions including France, Germany, Italy, Spain, Switzerland, and the Netherlands; non-European civil law jurisdictions including Brazil, Mexico, Japan, China, Russia, and South Africa; and Islamic countries and countries with large Muslim populations, including Pakistan, Indonesia, Malaysia, Nigeria, Ethiopia, Iran, and Turkey; (b) the November 2007 European Commission acknowledgement that “nearly all [EU

⁹² TURK. CRIM. CODE art. 221 [hereinafter TCK].

Member States] provide the possibility for the court judge to give a lighter punishment to offenders who help the police/judicial authorities to clarify their or other crimes" ([European Commission 2007](#)); (c) the fact that plea bargaining, penal orders, and related trial-avoiding conviction mechanisms are judicially recognized by high courts in 60 nations ([Langer 2021](#), Table 1); (d) the fact that plea bargaining is currently regulated and accepted in 27 European civil law countries ([Bicek 2022](#)); (e) the fact that sentence reduction for cooperating witnesses was endorsed by the member states of the European Union via the 2008 Framework decision of the European Council; (f) the December 2014 publication by the 46 member states of the Council of Europe, including France, Germany, Italy, and Spain, of a "white paper" on the topic of transnational organized crime noting that "the co-operation of insiders is crucial in investigating and combating [transnational organized crime]" ([Council of Europe 2014](#), p. 30) and urging states parties to consider "various forms of plea bargaining, pre-judicial co-operation agreements and summary prosecutions, as already used or being developed by a number of Council of Europe member states (e.g., Azerbaijan, Estonia, Switzerland, the UK)" ([Council of Europe 2014](#), pp. 31–32); (g) the fact that most Council of Europe states parties have measures of a generic nature in place (usually to be found in their criminal codes), permitting collaboration to be considered as a circumstance mitigating criminal liability and taken into account by the court during sentencing ([Council of Europe 2014](#), p. 31); (h) international instruments requiring that states parties take measures, in accordance with their fundamental legal principles, to encourage the cooperation of witnesses with law enforcement authorities, including UNTOC (Article 26) and the UN Convention against Corruption (UNCAC, Article 37), as well as the EU Council Resolution of 20 December 1996 on individuals who co-operate with the judicial process in the fight against international organized crime, and EU Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organized crime (Article 4); (i) a comparative analysis of legal regimes in the Netherlands, Germany, Italy and Canada that found that incentives to cooperate, involving reductions in sentences, i.e., "the granting of benefits in exchange for testimony in the prosecution of others" are legitimate and necessary ([Crijns et al. 2017](#), p. 324); and (j) the analysis in Section 3.12.4 indicating that there is nothing in Islamic law that is inconsistent with the application of plea bargaining, and cooperation agreements involving plea bargains, to violations of the proposed APUNCAC Beneficial Owner Rule.

The analysis in Section 3.12 suggests that cooperation agreements are compatible with civil, as well as common, law legal systems, are internationally accepted, and represent a promising strategy for fighting transnational organized crime. Bank clerks and front men represent ideal targets for cooperation agreements. Their crimes are not violent crimes. There are no victims' rights groups lobbying against the use of plea bargains and cooperation agreements with bank clerks and front men. There is general agreement that the cooperation of witnesses is key to the fight against organized crime. There is general agreement that bank clerks and front men are peripheral individuals who are manipulated by criminal masterminds who orchestrate criminal schemes, there is a need to prosecute the criminal masterminds, and it is acceptable for a prosecutor to exchange a reduced charge or suspended sentence for information or testimony leading to the conviction of the criminal masterminds. The acceptance of this practice is underlined by the review of both civil and common law legal systems in Section 3.12. The review established that charge reduction or immunity, in exchange for testimony leading to the prosecution of criminal masterminds, is judicially accepted across an array of civil and common law legal systems.

3.12.7. Implications

The preceding review of legal regimes established that cooperation agreements are, in most jurisdictions, a viable option and strategy for securing the cooperation of peripheral individuals such as bank clerks and front men. Cooperation agreements may be elicited by requesting states, involving individuals located in requested jurisdictions. For example, if Kenya is a party to the APUNCAC Rule, Kenya might seek a cooperation agreement with a bank clerk or front man located in BVI, the Caymans, Cyprus, or Malta. The Rule

would create the necessary extraterritorial regulation and control. Kenyan prosecutors might dangle the option of a cooperation agreement in lieu of extradition and prosecution in Kenya. This might be an attractive option for a bank clerk or front man who would otherwise risk imprisonment in Kenya.

The existence of criminal procedure codes that permit plea bargaining and the use of cooperation agreements would enable local prosecutors to gain the cooperation of bank clerks and front men whose testimony would be key in pursuing criminals who operate money laundering schemes. The widespread existence of laws permitting plea bargaining and the use of cooperation agreements across jurisdictions, including BVI, the Caymans, Cyprus, and Malta, implies that local prosecutors could utilize these provisions to secure the cooperation and testimony of bank clerks and front men.

3.13. High-Volume Transactions

Some entities conduct high-volume transactions. These entities could set an electronic flag on their accounts to indicate that the true beneficial owner certifies that he is the true beneficial sender of all funds transmitted from his accounts and he is the true beneficial recipient of all funds received by his accounts (Yeh 2022a, note 4).⁹³ Presumably, legitimate beneficial owners would not hesitate to name themselves as beneficial owners. This electronic flag would be read by a dedicated smartphone application when a transaction is initiated. This action could be performed digitally in milliseconds, eliminating transaction friction that might otherwise result from application of the Rule.

Suppose, for example, that a financial services provider transmits thousands of wire transfers to and from Cyprus every day involving a national of a State Party to the APUNCAC Beneficial Owner Rule. If the beneficial owners of the sending and receiving accounts have previously set electronic flags on their accounts certifying beneficial ownership of all funds transmitted from or received by those accounts, the flags would be read in milliseconds, meaning that certification would occur in milliseconds, and there would be little or no noticeable transaction delay.

The same digital technology enables high-speed, high-volume automatic credit card payments. Every day, vendors initiate millions of automated credit card charges that have been pre-authorized by the owners of the corresponding credit cards. Each transaction involves a complex series of digital electronic communications involving the merchant, payment gateway, credit card issuing bank, and acquiring bank that processes credit or debit card payments on behalf of the merchant. However, modern digital technology permits these communications to be completed in milliseconds. The same technology would permit high-speed, high-volume beneficial owner certification.

The digital communication technology required to collect and report beneficial owner information already exists. In June 2019, FATF implemented a requirement that virtual asset service providers (VASPs)—i.e., entities that exchange virtual assets such as cryptocurrency for fiat currencies or other forms of virtual assets or transfer virtual assets from one person to another—implement the “travel rule” (FATF 2019b). The purpose of the rule is to fight money laundering. The rule requires VASPs to collect and record the identities of the sender and recipient of cryptocurrency when a transaction is conducted in cryptocurrency.

The rule requires “originating VASPs” to “obtain and hold required and accurate originator information and required beneficiary information” and submit the information to “the beneficiary VASP”.⁹⁴ The rule requires “beneficiary VASPs” to “obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities”.⁹⁵ For example, a VASP that originates a Bitcoin transaction must obtain accurate customer identity information from the originator of the transaction and must transmit the infor-

⁹³ APUNCAC arts. 21(2)(a)(H)(7), 21(3)(a)(viii)(G), 21(3)(b)(viii)(G), 22(1)(a)(G)(7), 30(b)(7).

⁹⁴ *Id.*

⁹⁵ *Id.e*

mation to the beneficiary VASP. In turn, the beneficiary VASP must obtain and hold the required originator information as well as required and accurate information regarding the beneficiary.

In response, CoolBitX developed and introduced Sygna Bridge, a digital travel rule solution (CoolBitX 2020a, 2020b). The product enables VASPs to comply with the FATF travel rule by using digital technology to collect and exchange the identities of the sender and receiver involved in a virtual asset transaction. The solution demonstrates the technological feasibility of collecting and securely transmitting high volumes of the type of customer identity information envisioned by the APUNCAC Beneficial Owner Rule.

A customized digital application may be designed to electronically package the required APUNCAC Beneficial Owner Rule information regarding each transaction together with a certification of beneficial ownership, then transmit the information to a designated FINCEN database. In any context where a customer is using an account suitable for using an electronic flag, existing data input systems may be adapted to collect the required information, pre-fill the electronic certifications, and automate the entire certification process, eliminating transaction friction. This includes the data input systems at all types of financial institutions, money transmitters, and retail vendors.

To establish an account at, for example, a money transmitter, certain information is required. This system could be modified to collect the information required to implement automated, flag-based, beneficial owner certification in accordance with the proposed Rule. If the system is computer-based, the change would involve a software update. Once the system is modified, there would be little or no increase in transaction friction.

If a beneficial owner chose the option of one-time certification of beneficial ownership by the beneficial owner of all funds sent or received from the owner's account, the previously collected information would be converted into a digital representation suitable for automated, high-speed transmission. The certification would involve digital boilerplate language with the details of each transaction. The digital application would, for each transaction, automatically fill the name of the beneficial owner, a code for the source of the funds, and the beneficial owner certification. This would obviate the need for manual entry of the information, permit high-speed, automated certification of beneficial ownership, and eliminate transaction friction.

3.14. Rural Areas

A concern is that digital technology may not be available in rural areas, especially in developing nations. However, 3G network coverage exceeds 80 percent of the sub-Saharan African population (GSMA 2022, Figure 14). Only 20 percent of the sub-Saharan population lacks access to a 3G network—presumably, the poorest 20 percent. However, that segment of the African population does not possess the wealth to engage in covered transactions. These individuals would be unaffected by the Rule. The median annual income in sub-Saharan Africa is USD 1044, i.e., half of the population earns less than USD 1,044 per year (University of Oxford 2023). It is extremely unlikely that any person earning less than USD 1044 per year would conduct a cash transaction in an amount of USD 3000 or more that would be subject to the Rule. Median annual income is USD 1310 in rural India, USD 1467 in South Asia, USD 1865 in rural Indonesia, USD 2745 in the Middle East/North Africa region, and USD 2957 in rural China (University of Oxford 2023). It is extremely unlikely that a person in any of these regions who falls in the bottom half of the income distribution would not have access to a 3G network yet conduct a cash transaction in an amount of USD 3000 or more that would be subject to the Rule. For these individuals, the threshold is above their annual income. It is unlikely that they would seek to transfer an amount greater than their entire annual income in a single lump sum. Anyone who chooses to do so would have access to the necessary technology by traveling to a town of sufficient size.

Conceptually, all beneficial owners, including customers in rural areas, may be divided into two categories. Beneficial owners who engage in covered transactions typically have access to and utilize financial accounts suited to the use of electronic flags. They typically

have access to smartphone technology and are familiar with that technology. They have access to money transmitters with access to smartphones.

Anyone who does not have ready access to financial accounts suited to the use of electronic flags, e.g., farmers in rural areas, would typically need to travel to a town of sufficient size to engage the services of a money transmitter or to conduct a purchase or sale involving an amount above USD 3000, regardless of the implementation of the Rule. It would be necessary to travel to town simply to gain access to a suitable vendor or money transmitter. There, they would have access to a vendor or money transmitter with access to smartphone technology, knowledge of the technology, and access to the internet. But the trip to town would be required regardless of the Rule because money transmitters and vendors who engage in large cash transactions are concentrated in towns, not isolated rural areas. In sum, the additional transaction friction created by the implementation of the Rule would be relatively minor.

In rural areas, it is not unusual for customers to send or receive funds via money transmitters without establishing an account with a transmitter. Customers who choose this option would experience transaction friction, but that would be a deliberate choice, akin to using snail mail (paper mail) instead of email, despite the availability of email. For example, a customer may choose to send money via a money transmitter such as MoneyGram without establishing an account or may choose to establish a MoneyGram account for the purpose of sending money (Melendez 2019). If a customer chose the former option, it would not be possible to set an electronic flag. The customer would, under the Rule, be required to certify beneficial ownership for each transaction exceeding USD 3000. If, however, the customer chose the latter option, it would be possible to set an electronic flag that would automatically certify beneficial ownership, thereby obviating the need to manually certify beneficial ownership for each individual transaction exceeding USD 3000. This would eliminate transaction friction at the customer's end of the transactions.

Customers in rural areas lacking access to electronic communications would not have access to this convenience. But since they would, regardless of the Rule, be forced to travel to a town whenever they wish to engage the services of a money transmitter, the additional transaction friction created by the implementation of the Rule would be relatively minor.

3.15. No Electricity/No Internet

If an electrical or internet outage prevents digital certification at the point of a transaction, the transaction may proceed, contingent upon digital certification, when electricity or internet is restored. FINCEN could specify a time period, e.g., 48 h. Digital certification would be required within this time period. Upon expiration of this time period, transactions lacking certification would be reversed. Failure to reverse a transaction would entail the same penalties and consequences that would be entailed for any covered transaction conducted without the required certification.

3.16. Transactions Involving Agents

Some beneficial owners rely upon agents to conduct transactions on their behalf. This practice is not illegal. However, the APUNCAC Rule would impose a beneficial owner certification requirement that does not currently exist. The Rule would not permit agents to falsely certify beneficial ownership. The Rule would allow a principal to authorize an agent to submit the principal's beneficial owner certification but specifies that a principal who authorizes an agent to do this would be responsible in the same way that the principal would be responsible if he performed the certification in person.⁹⁶ For example, a principal may authorize a Trust or Company Service Provider (TCSP) to open a bank account and send and receive funds. The principal may authorize TCSP personnel to certify that the principal is the true beneficial owner. However, false statements would entail the same

⁹⁶ *Id.* arts. 21(2)(a)(H)(3), 21(2)(a)(H)(4), 21(3)(a)(viii)(C), 21(3)(a)(viii)(D), 21(3)(b)(viii)(C), 21(3)(b)(viii)(D), 22(1)(a)(G)(3), 22(1)(a)(G)(4), 30(b)(3), 30(b)(4).

penalties for the principal that would apply had the principal made the false statements in person. Principals may not escape the consequences of false assertions regarding beneficial ownership merely by inserting agents who are authorized to act on their behalf.

The current practice of allowing agents to conduct transactions in their own names without submitting certifications of beneficial ownership serves to obscure the origin and nature of funds that may be illicit.

3.17. Privacy Concerns

With respect to beneficial owner reporting requirements, regulators have already decided that the public interest in controlling money laundering outweighs privacy concerns. FATF recommendations state that information regarding beneficial ownership should be collected and recorded for the purpose of detecting and deterring money laundering (FATF 2014).

While some customers may, for privacy reasons, prefer to avoid the application of the Rule, these individuals may do so by using a credit card, debit card, personal check (not in bearer form), mobile payment (not involving cryptocurrency), or ACH. These forms of payment provide investigators with a digital trail, are less likely to be used for money laundering, and are not covered by the Rule. The Rule may be expected to promote the use of these forms of payment in lieu of currency transactions. The burden of the Rule would fall on individuals who insist on cash transactions exceeding USD 3000 or insist on sending funds to high-risk jurisdictions such as Panama, the Cayman Islands, or the British Virgin Islands.

3.18. Exempt Transactions

Certain transactions involving banks are exempt from the Rule.⁹⁷ The exemptions are modeled on the exemptions to the U.S. Treasury Department's currency transaction reporting rule. This eliminates transaction friction that might otherwise hinder entities unlikely to be involved in money laundering.

3.19. Anonymous Instructions

The APUNCAC Beneficial Owner Rule prohibits anonymous instructions to an agent.⁹⁸ The person who gives instructions cannot hide behind pseudonyms or anonymous emails. The use of pseudonyms or anonymous emails is an obvious violation of the Rule that would be punishable by debarment, fines, or imprisonment. When the individual who gives instructions is unable to hide behind pseudonyms or anonymous emails, those instructions reveal the person controlling the transaction, i.e., the true beneficial owner.

3.20. Structuring

The Rule prohibits structuring, i.e., structuring a series of transactions for the sole purpose of avoiding the Rule, e.g., in amounts just below the USD 3000 threshold.⁹⁹

3.21. Beneficial Owner Is Not a Natural Person

When no natural person directly or indirectly exerts more than 25 percent control, the Rule specifies that a principal of the entity transmitting the funds must certify that statement under penalty of perjury.¹⁰⁰ If a front man falsely certifies that no natural beneficial owner exists, a prosecutor who obtains incriminating evidence, e.g., in the form of text messages directing the front man to send or receive funds, may prosecute the front man for perjury, and may prosecute any individual who directs the front man for the crime of aiding and abetting a criminal scheme.

⁹⁷ *Id.* art. 31.

⁹⁸ *Id.* art. 19(6).

⁹⁹ *Id.* art. 32.

¹⁰⁰ *Id.* arts. 21(2)(a)(H)(2), 21(3)(a)(viii)(B), 21(3)(b)(viii)(B), 22(1)(a)(G)(2), 30(b)(2).

3.22. *Prohibition against Aiding and Abetting*

The Rule specifies that no person may aid or abet a scheme to hide the identity of the true beneficial owner controlling a transaction.¹⁰¹ This would apply to any individual who directs a front man to send or receive funds. This action serves to aid and abet a criminal scheme where the front man falsely certifies that he is the true beneficial owner controlling a transaction but is not, in fact, the person controlling the transaction. This opens the door for a prosecutor to pressure each individual involved in the scheme to cooperate, provide useful information about other individuals involved in the conspiracy, and thereby permit the prosecutor to work his way up the chain toward the individual who truly controls the transaction.

3.23. *Penalties*

Under the APUNCAC Rule, debarment, fines, or a term of imprisonment not to exceed five years would be imposed on individuals who fail to obtain and submit beneficial owner certification and front men who falsely certify beneficial ownership.¹⁰² This would discourage large-scale assistance by the army of facilitators (e.g., bank clerks and front men) required to launder dirty money. No facilitator would be safe from extradition and prosecution. Many facilitators would choose to exit the profession of money laundering because the risks would outweigh the rewards. Facilitators who are convicted would face a choice: cooperate and testify against the criminals who orchestrate the criminal activity or face long prison terms.

A first offense would be punishable by debarment, where an offender would be debarred from participating in, or assisting with, specified transactions, or serving as a director, partner, or trustee for a legal entity. Additional offenses would be punishable by a term of imprisonment not to exceed five years or a fine of USD 250,000. This would deter participation in money laundering schemes.

3.24. *Enforcement*

Enforcement would depend upon the willingness of a core group of nations to implement the APUNCAC Rule. This type of extraterritorial financial regulation is not uncommon (see Section 3.31, below). The six examples described in Section 3.31 and the six examples described in Section 3.32 of multilateral agreements to collect, report, and exchange beneficial ownership information signal international consensus that the benefits exceed the costs of this type of regulation. It is not unreasonable to think that a core group of nations would agree to implement the APUNCAC Rule.

If a core group of nations adopts and implements the APUNCAC Rule, the offenses established by the Rule would be established in the criminal codes of those nations. The APUNCAC Rule would be an internal domestic requirement written into the criminal legal code of all APUNCAC jurisdictions. In cases of extradition between APUNCAC States Parties, the Rule would have the force of law, would govern behavior in both jurisdictions and would be judicially accepted in both jurisdictions. The validity of the Rule for the purpose of extradition would be unquestioned. Satisfaction of the dual criminality requirement would permit extradition from one APUNCAC State Party to another. The dual criminality requirement—perhaps the main barrier to extradition—would be overcome. Once extradition had been obtained, prosecution would proceed.

Satisfaction of the dual criminality requirement would enable APUNCAC States Parties to rely upon the application of existing extradition treaties or the extradition provisions of UNTOC to extradite individuals who violate the Rule (Yeh 2020a, pp. 152–58). Globally, all but six minor jurisdictions are parties to UNTOC. The only United Nations Member States that are not parties are Bhutan, Papua New Guinea, the Solomon Islands, Somalia, South Sudan, and Tuvalu (see United Nations 2023). Thus, APUNCAC States Parties

¹⁰¹ *Id.* art. 19(6).

¹⁰² *Id.* arts. 39, 40.

would almost certainly be a subset of UNTOC States Parties, eligible to avail themselves of UNTOC's extradition provisions (Figure 7). A Panamanian bank clerk who violated the Rule and traveled to an APUNCAC jurisdiction would risk extradition for violating a law that requires the bank clerk to obtain and submit beneficial owner certification. Awareness of this possibility would deter violations by bank clerks in all jurisdictions, including states that reject the APUNCAC Rule. In this way, a State Party to the Rule could apply the Rule to exert extraterritorial control over financial service personnel in distant offshore havens at the point when they handle covered funds.

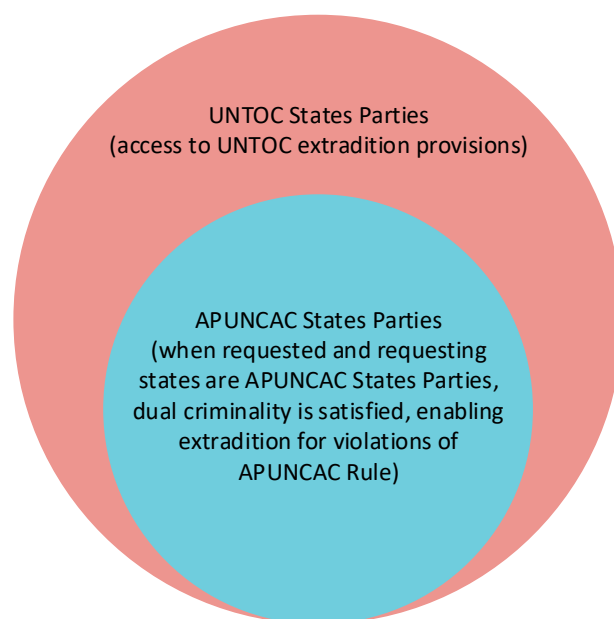


Figure 7. APUNCAC States Parties would be a subset of UNTOC States Parties.

Failure to observe the Rule would create a risk of extradition if and when those personnel travel for business or leisure to an APUNCAC jurisdiction (Yeh 2020a, pp. 152–58) (Figure 8). Presumably, financial service personnel would avoid employment in recalcitrant jurisdictions or with recalcitrant entities that decline to observe the Rule. This would create pressure to observe the Rule.

Yeh (2020a) explained how UNTOC, in combination with the Rule, would be applied to exert extraterritorial jurisdiction:

[UNTOC] criminalizes “the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime” as well as “participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating” such concealment.¹⁰³ UNTOC makes these offenses “an extraditable offence in any extradition treaty existing between States Parties”.¹⁰⁴ Furthermore, “States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them”.¹⁰⁵ UNTOC requires States Parties to implement requirements for customer identification and record-keeping to deter and detect money laundering:

¹⁰³ *Id.* art. 6(1).

¹⁰⁴ *Id.* art. 16(3). Significantly, 190 nations are parties to UNTOC. The only United Nations Member States that are not parties are Bhutan, Papua New Guinea, the Solomon Islands, Somalia, South Sudan, and Tuvalu. This implies that extradition for offenses covered by UNTOC is available to all nations except these six states.

¹⁰⁵ *Id.* art. 16(3).

Each State Party: (a) Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions;¹⁰⁶

These provisions apply to nationals and residents of all States Parties. They apply to bank clerks in the British Virgin Islands, the Cayman Islands, or Panama who aid, abet and facilitate the concealment of the true ownership of illicit funds, because Panama, the United Kingdom, and its possessions are parties to UNTOC. A bank clerk who is required to perform, but chooses to willfully, intentionally, and knowingly ignore basic steps designed to identify customers and promote transparency in the ownership, disposition and movement of property and permit verification of the legitimacy of such property could be found guilty under UNTOC of aiding, abetting and facilitating the concealment of the true nature, source and ownership of that property. (Yeh 2020a, pp. 152–53)

The beneficial owner identification and recordation provisions of the [APUNCAC Beneficial Owner Rule] are precisely “requirements for customer identification [and] record-keeping” with the exact intention of deterring and detecting money-laundering.¹⁰⁷ The beneficial owner identification and recordation provisions would plug holes in existing customer identification requirements by requiring each banking customer to identify the beneficial owner of funds that are deposited in currency, deposited in any form in a high-risk jurisdiction, or transmitted internationally by wire from the territory of a state party.¹⁰⁸ The model protocol serves to translate the existing legal commitment of UNTOC parties to identify banking customers for the purpose of revealing the true “ownership of or rights with respect to property” into specific procedures for identifying beneficial owners, for that exact purpose.¹⁰⁹ The model protocol seeks to achieve UNTOC’s goal of establishing the identities of true owners by specifying that banking customers must certify the identities of true beneficial owners under penalty of perjury.¹¹⁰ An argument that non-State Party nationals (perhaps bank clerks in the British Virgin Islands, Cayman Islands, or Panama) would not be legally obligated to observe the model protocol’s beneficial owner identification requirement is inconsistent with and contradicts the existing legally binding commitment of UNTOC parties to identify the true identities of banking customers. This argument denies the legally binding commitments that have already been made to require customer identification and record-keeping for the purpose of deterring and detecting money-laundering. (Yeh 2020a, pp. 153–54)

UNTOC obligates all States Parties to extend the maximum level of cooperation regarding requests for mutual legal assistance and to cooperate, to the extent permitted by domestic law, with extradition requests regarding violations of these requirements.

UNTOC is a powerful mechanism to achieve extradition. A core group of nations that agrees to implement the APUNCAC Rule could utilize UNTOC to extradite violators of the Rule who are found in an APUNCAC State Party jurisdiction. If a national of a state that is not a party to APUNCAC entered the jurisdiction of an APUNCAC State Party—on business or leisure—that person could be extradited. This risk would tend to

¹⁰⁶ *Id.* art. 7(1).

¹⁰⁷ *Id.* art. 7(1).

¹⁰⁸ APUNCAC arts. 21(2), 22(1), 30.

¹⁰⁹ UNTOC art. 6(1).

¹¹⁰ APUNCAC arts. 21(2), 22(1), 30.

deter violations of the Rule in all jurisdictions, including states that were not parties to the APUNCAC Rule. The combination of the APUNCAC Rule plus UNTOC would create a powerful mechanism to ensure that the true beneficial owner is properly identified for all covered transactions. Violations of the Rule would give prosecutors opportunities to pressure violators into cooperation agreements where they would provide the information and testimony necessary to convict criminals who orchestrate criminal schemes involving violations of the APUNCAC Rule. This mechanism would deter money laundering and the crime associated with money laundering.

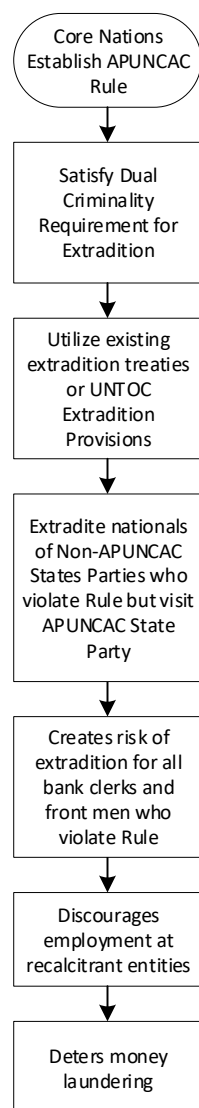


Figure 8. Violations of APUNCAC Rule create risk of extradition.

3.25. Extradition

Modern extradition arrangements “are designed to promote extradition” (Seddon et al. 2021, p. 570). Swift decision-making and consistency are promoted via bilateral and multilateral agreements that simplify and formalize the requirements for extradition. Increasingly, time limits imposed via domestic law attach to the various procedural stages of an extradition hearing (see Seddon et al. 2021, p. 570). Extradition requests are moving through the courts increasingly swiftly, facilitated by judicial precedents that inform subsequent decisions, promote clarity in decision-making, and reduce legal and procedural uncertainties (see Seddon et al. 2021, p. 570).

Not only have the numbers of extradition cases increased exponentially in recent years, but the decision to extradite, in EU states and the UK, is now almost always made by a court rather than the executive (Seddon et al. 2021, p. 568). “Decisions as to whether to extradite a requested person are now made upon the basis of an established and well-defined set of rules, in an open and public forum, by tribunals whose decisions can be challenged in superior courts” (Seddon et al. 2021, p. 568). Where the executive retains a role in the process, that role is heavily circumscribed (Seddon et al. 2021, pp. 568–69). There is little or no room for the government to depart from court-sanctioned procedures, standards, and criteria (see Seddon et al. 2021, p. 569). This promotes consistency and limits the degree to which extradition decisions are politicized.

UNTOC is designed to facilitate international cooperation, mutual legal assistance, and extradition in regard to all kinds of serious crimes where there is a cross border element (Boister 2016, pp. 45–47). In resolution 2009/22 of July 30, 2009, the UN Economic and Social Council (ECOSOC) mentioned the importance of UNTOC in preventing and combating economic fraud and identity-related crime.¹¹¹ In resolution 2007/20 of 26 July 2007, the Council extended the scope of the language used in its resolution 2004/26 of 21 July 2004, and encouraged “Member States to take into account the use of terms and scope of application set out in articles 2 and 3 of the United Nations Convention against Transnational Organized Crime in establishing or updating, as appropriate, offenses relating to the criminal misuse and falsification of identity”.¹¹² UNTOC has been used as the basis for requesting international criminal law assistance in an investigation of “the offense of misrepresentation”, i.e., a crime parallel to a violation of the APUNCAC Rule involving misrepresentation of beneficial ownership.¹¹³ Another case involved fraudulent documents, i.e., a crime parallel to a false certification of beneficial ownership that would be a violation of the APUNCAC Rule.¹¹⁴ In at least 13 cases, requests for extradition under UNTOC Article 16 were made alongside existing bilateral extradition treaties between the requesting and requested States (UNODC 2021, p. 107). Extraditable offenses under these bilateral treaties generally included the full range of criminal offenses (UNODC 2021, p. 107).

UNTOC defines a serious crime as an offense punishable by a maximum term of imprisonment of at least four years.¹¹⁵ UNTOC’s scope of application is serious crime where the offense is transnational in nature and involves a criminal group, “except as otherwise stated herein”.¹¹⁶ Significantly, UNTOC permits a State Party to assert jurisdiction, according to the effects principle, over the crime of aiding, abetting, facilitating or counselling the commission of serious crime involving an organized criminal group “committed outside its territory with a view to the commission of a serious crime within its territory”.¹¹⁷ A State Party to UNTOC that asserts jurisdiction regarding offshore enablers and facilitators of money laundering may rely upon UNTOC, a binding international agreement, to reject attacks on that assertion.

Other extradition agreements simplify extradition procedures. For example, the Caribbean Community (CARICOM) Arrest Warrant Treaty establishes, within the Caribbean Community, a system of arrest and surrender of requested persons for purposes of criminal

¹¹¹ Conference of the Parties to the UNTOC, “The Notion of Serious Crime in the United Nations Convention against Transnational Organized Crime”, CTOC/COP/2012/CRP.4 (20 September 2012), para. 30.

¹¹² *Id.*

¹¹³ Conference of the Parties to the UNTOC, “Catalogue of Cases Involving Extradition, Mutual Legal Assistance and Other Forms of International Legal Cooperation Requested on the Basis of the United Nations Convention against Transnational Organized Crime”, para. 73, CTOC/COP/2010/CRP.5 (22 September 2010).

¹¹⁴ *Id.* para. 50.

¹¹⁵ UNTOC art. 2(b).

¹¹⁶ *Id.* art. 3(1)(b) (“This Convention shall apply, except as otherwise stated herein, to the prevention, investigation and prosecution of serious crime as defined in article 2 of this Convention; where the offence is transnational in nature and involves an organized criminal group”).

¹¹⁷ *Id.* art. 15(2)(c)(i).

prosecution.¹¹⁸ Dual criminality is not a requirement for extradition for listed offenses including “false statement”, “obtaining... money... by false pretence or other forms of deception”, “fraud, including fraud against the government... including behavior which has the effect of depriving the Government, its agencies, or its citizens of money, valuable property, or the ability to conduct their affairs free from false statements and deceit”, and “attempting to pervert or obstruct the course of justice”, as well as aiding and abetting those offenses.¹¹⁹

This provision implies that dual criminality would not be required for violations of the APUNCAC Rule, including a false certification of beneficial ownership (i.e., a false statement) or failure of a bank clerk to obtain and submit a certification of beneficial ownership required by the Rule (i.e., deprivation of government ability to implement its customer due diligence AML regulations free from the type of false statements and deceit that occurs when customer due diligence requirements are not observed, obstructing justice by obstructing a lawful regulation, and aiding and abetting those offenses). A CARICOM Arrest Warrant may be issued for the arrest and surrender of a person who is “reasonably suspected of having committed an applicable offense”.¹²⁰ Notably, “a CARICOM Arrest Warrant shall be dealt with and executed as a matter of urgency”.¹²¹ CARICOM allows an arrest warrant backed by the signature of a judge to be the basis of a request to another country (West 2019, p. 394). On receipt of the arrest warrant, the person wanted would be arrested, taken before a magistrate and returned to the requesting State (West 2019, p. 394). There is no requirement for formal authenticated evidence (West 2019, p. 394). In principle, CARICOM would permit extradition for violations of the APUNCAC Rule.

The Extradition Act 2003 (Overseas Territories) Order 2016 simplifies extradition from British overseas territories including Anguilla, Bermuda, Cayman Islands, Saint Helena, Turks and Caicos Islands, and Virgin Islands, to 148 jurisdictions including the Bahamas, Botswana, Colombia, Cyprus, Estonia, Ghana, Kenya, Lesotho, Liberia, Malawi, Malaysia, Malta, Mexico, Sierra Leone, South Africa, Tanzania, Uganda, Zambia, and Zimbabwe.¹²² The requesting jurisdiction would issue a request for arrest and extradition of an accused person, for the purpose of prosecution.¹²³ A prosecutor in the requested territory must certify that one or more offenses within the territory “correspond to the extradition offense”.¹²⁴ An “appropriate judge for the extradition hearing” would decide whether “the offense specified in the request is an extradition offense”.¹²⁵ A judge may bar extradition “if the extradition would not be in the interests of justice”.¹²⁶ A judge may consider “the place where most of the loss or harm resulting from the extradition offense occurred or was intended to occur”, “the interests of any victims of the extradition offense”, “any belief of a prosecutor that the Territory is not the most appropriate jurisdiction in which to prosecute”, and “the desirability and practicability of all prosecutions relating to the extradition offence taking place in one jurisdiction”.¹²⁷ In principle, the Order would facilitate extradition for violations of the APUNCAC Rule.

¹¹⁸ CARICOM Arrest Warrant Treaty, opened for signature 5 July 2017 (entered into force 20 July 2018) [hereinafter CARICOM AWT]. Parties include the Bahamas, Barbados, Dominica, Grenada, Guyana, Jamaica, St. Kitts and Nevis, Saint Lucia, and Trinidad and Tobago.

¹¹⁹ *Id.* art. 3(3), Annex II, A(11), A(22), A(24), B.

¹²⁰ *Id.* art. 4(a).

¹²¹ *Id.* art. 10(1).

¹²² The Extradition Act 2003 (Overseas Territories) Order 2016, scheds. 1–2, S.I. 2016, No. 990 [hereinafter Extradition (Overseas Territories) Order 2016].

¹²³ *Id.* § 70(4)(b).

¹²⁴ *Id.* § 83C(3) [“the responsible prosecutor has decided that there are one or more such offences that correspond to the extradition offence (the ‘corresponding offences’)”].

¹²⁵ *Id.* § 78(4), as modified at 75 (“The judge must decide whether the offense specified in the request is an extradition offense”).

¹²⁶ *Id.* § 83A(1).

¹²⁷ *Id.* § 83A(3).

The London Scheme, introduced in 1966, simplifies the extradition of individuals among 56 Commonwealth Nations.¹²⁸ Under the London Scheme, extradition is possible for offenses punishable, in both the requesting and requested state (the dual criminality requirement), by imprisonment for two years or more. Offenses included within the London Scheme are crimes committed outside of the requesting state, which constitute extraditable offenses in the requested state (Peters and Peters n.d.). Commonwealth Nations include: Antigua and Barbuda, Australia, The Bahamas, Bangladesh, Barbados, Belize, Botswana, Brunei, Cameroon, Canada, Cyprus, Dominica, Fiji, Gabon, Gambia, Ghana, Grenada, Guyana, India, Jamaica, Kenya, Kingdom of Eswatini, Kiribati, Lesotho, Malawi, Malaysia, The Maldives, Malta, Mauritius, Mozambique, Namibia, Nauru, New Zealand, Nigeria, Pakistan, Papua New Guinea, Rwanda, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Samoa, Seychelles, Sierra Leone, Singapore, Solomon Islands, South Africa, Sri Lanka, Swaziland, Tanzania, Tonga, Trinidad and Tobago, Tuvalu, the United Kingdom, Uganda, Vanuatu and Zambia.

In the U.S., the general procedure is as follows¹²⁹:

First, the foreign state seeking extradition makes a request directly to the U.S. Department of State (“State Department”). If the State Department determines that the request falls within the operative extradition treaty, a U.S. Attorney files a complaint in federal district court indicating an intent to extradite and seeking a provisional warrant for the person sought. And once the warrant is issued, the district court—which could include a magistrate judge—conducts a hearing. This hearing is to determine whether there is evidence sufficient to sustain the charge under the operative treaty, i.e., “whether there is probable cause”. See *Santos*, 830 F.3d at 991 (citing 18 U.S.C. § 3184; *Vo v. Benov*, 447 F.3d 1235, 1237 (9th Cir. 2006)). Of note, the hearing to determine probable cause is “akin to a grand jury investigation or a preliminary hearing under Federal Rule of Criminal Procedure 5.1”. *Id.* (citations omitted). If the court (including the magistrate judge) determines there is probable cause, the court “is required to certify the individual as extraditable to the Secretary of State”. *Vo*, 447 F.3d at 1237 (emphases removed) (quoting *Blaxland v. Commonwealth Dir. Of Pub. Prosecutions*, 323 F.3d 1198, 1208 (9th Cir. 2003)). Upon certification, the Secretary of State decides whether to extradite the individual, the final decision being discretionary. See *id.* (citations omitted). See generally FJC Manual at iv (“Overview of the Extradition Process”).

The key is whether the evidence presented by the foreign government is “sufficient to sustain the charge under the provisions of the proper treaty or convention”.¹³⁰ The demanding country is permitted to introduce properly authenticated evidence collected there; “a fugitive’s right to introduce evidence is ‘limited to testimony which explains rather than contradicts the demanding country’s proof’”.¹³¹ Furthermore, the evidence at the extradition hearing may consist of unsworn statements and hearsay evidence.¹³² A certificate of extradition will ultimately be issued if competent evidence is presented sufficient to establish probable cause that the fugitive committed the alleged offense.¹³³

¹²⁸ The London Scheme for Extradition within the Commonwealth (amended) [hereinafter London Scheme].

¹²⁹ *Bowman v. Stafford*, No. 20-cv-2250-GPC-MSB, 2022 WL 118227, at *1 (SD Cal. 12 January 2022).

¹³⁰ 18 USC § 3184.

¹³¹ *Sandhu v. Bransom*, 932 F. Supp. 822, 827 (ND Tex. 1996). See generally Roberto Iraola, “Contradictions, Explanations, and the Probable Cause Determination at a Foreign Extradition Hearing”, *Syracuse Law Review* 60: 95–124 (2009), p. 95 (discussing the “Rule of Non-Contradiction” which governs foreign extradition hearings).

¹³² See *Collins v. Loisel*, 259 US 309, 317 (1922) (“[U]nsworn statements of absent witnesses may be acted upon by the committing magistrate, although they could not have been received by him under the law of the State on a preliminary examination.”); *Artukovic v. Rison*, 784 F.2d 1354, 1356 (9th Cir. 1986) (“[U]nsworn hearsay statements contained in properly authenticated documents can constitute competent evidence to support a certificate of extradition.”). See also *In re Extradition of Luna-Ruiz*, No. CV 13-5059 VAP AJW, 2014 WL 1089134, at *4 (C.D. Cal. 19 March 2014) (collecting cases), *aff’d sub nom.* *Luna-Ruiz v. Barr*, 753 F. App’x 472 (9th Cir. 2019).

¹³³ See, e.g., *Mironescu v. Costner*, 480 F.3d 664, 665 (4th Cir. 2007) (identifying factors).

The ‘probable cause’ threshold for extradition is relatively low, implying that extradition under UNTOC would be a genuine threat to individuals who violate the APUNCAC Rule.

The Secretary of State would review the case and determine whether to issue a surrender warrant for the fugitive.¹³⁴ While extradition may be refused for humanitarian or foreign policy reasons, these reasons would be inapplicable for violations of the APUNCAC Rule.¹³⁵

Applicable extradition agreements such as the CARICOM Arrest Warrant Treaty, the Extradition Act 2003 (Overseas Territories) Order 2016, and the London Scheme can be used together with the extradition provisions of UNTOC when a requesting state requests extradition from a requested state. These agreements illustrate how extradition may be obtained, for example, from offshore havens to African countries that have been victimized by corrupt individuals. Section 3.25 draws upon these agreements and provisions to illustrate multiple paths that a prosecutor may pursue to achieve extradition and prosecution.

3.25.1. Definitions

UNTOC defines a transnational offense to include an offense “committed in one State but has substantial effects in another State”.¹³⁶ “The mere fact that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State party constitutes in itself sufficient reasonable grounds to suspect that the offence is transnational in nature” (UNODC 2021, p. 38).¹³⁷ Notably, “[a]lthough the focus of the Convention is on transnational organized crime, according to Article 34, paragraph 2, national laws criminalizing the laundering of criminal proceeds (Article 6), corruption (Article 8) or obstruction of justice (Article 23) and the various Protocol offences shall be established independently of the transnational nature or the involvement of an organized criminal group”.¹³⁸ “National laws criminalizing participation in an organized criminal group (article 5) should not require the conduct to be transnational in nature”.¹³⁹ Article 16, regarding extradition, also applies to a serious crime involving an organized crime group, where “the person who is the subject of the request for extradition is located in the territory of the requested State Party”. This implies that the condition of transnationality of the offense, as described in Article 3, paragraph 2, is not strictly necessary for the application of Article 16.¹⁴⁰

UNTOC defines a criminal group as “a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes. . . in order to obtain, directly or indirectly, a financial or other material benefit”.¹⁴¹ UNTOC defines a structured group to “mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure”.¹⁴² UNTOC “is a remarkably flexible instrument with a very low threshold set of conditions” that trigger “its operation in the ‘prevention, investigation and prosecution’ of UNTOC’s specific crimes and serious crimes” (Boister 2016, p. 45).

¹³⁴ See 18 USC § 3184 (Judicial officer “shall certify the same . . . to the Secretary of State, that a warrant may issue. . . for the surrender of such person.”); § 3186 (“The Secretary of State may order the person committed under section 3184. . . to be delivered to any authorized agent of such foreign government”).

¹³⁵ Mironescu, 480 F.3d at 666; see also *Lo Duca v. United States*, 93 F.3d 1100, 1103–4 (2d Cir. 1996) (“[T]he Secretary of State has final authority to extradite the fugitive, but is not required to do so. Pursuant to its authority to conduct foreign affairs, the Executive Branch retains plenary discretion to refuse extradition”).

¹³⁶ UNTOC art. 3(2)(d).

¹³⁷ The Notion of Serious Crime at 4.

¹³⁸ *Id.* para. 12.

¹³⁹ *Id.*

¹⁴⁰ *Id.* para. 14.

¹⁴¹ UNTOC art. 2(a).

¹⁴² *Id.* art. 2(c).

3.25.2. Extradition Thresholds

Most extradition treaties, including the extradition provisions of UNTOC, require dual criminality, i.e., the offense for which extradition is requested must be criminalized by the requested state as well as the requesting state. Extradition is available for offenses covered by UNTOC, “provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party”.¹⁴³ Therefore, the APUNCAC strategy of enforcing the APUNCAC Rule on bank clerks requires that the requested State, as well as the requesting State, implement the APUNCAC Rule into domestic law. Dual implementation is needed to satisfy the dual criminality extradition requirement and enable extradition for violations of the Rule.¹⁴⁴

While dual criminality is generally required to obtain extradition, van der Wilt notes that a strict congruence of the elements of the offense is not required: “It is generally acknowledged that strict congruence of the elements of the offence in both jurisdictions is outdated and no longer required” (van der Wilt 2022, p. 33). Instead, the key is whether the elements of the offense are satisfied in the requested state. “In the case of *Nielsen* the House of Lords argued that, in extradition proceedings, it was paramount to inquire whether the conduct qualified as a crime under the law of the requested state” (van der Wilt 2022, p. 34).¹⁴⁵ Accordingly, a front man who falsely certified beneficial ownership could be extradited from England for the offense of perjury if the elements of the offense were satisfied in England.

If dual criminality is satisfied, and if an accused person travels outside his national territory, the nationality of the person, for the purpose of extradition, is irrelevant. A bank clerk or front man who is a national of a state that is not a party to the APUNCAC Rule (perhaps Panama) may be extradited for violations of the APUNCAC Rule once he travels (for business or leisure) to another state. Once an accused person leaves his national territory, he loses any protection from extradition afforded by his nationality. “Public international law generally forbids a state to claim jurisdiction”—or assert the protections of jurisdiction—“in a way that would interfere with the ability of another state to deal with third states or their nationals” (Gallant 2022, p. 554). If, for example, a Panamanian national traveled to Spain, Spain may choose to honor an extradition request by Kenya. International law does not permit Panama to protect its national once that person leaves Panamanian territory.¹⁴⁶

The international legality of the APUNCAC Rule is addressed in Sections 3.29 and 3.30, below. Once the legality of the Rule is accepted, the issue is whether a national of a state that is not a party to the APUNCAC Rule, e.g., a bank clerk or front man who violates the Rule in a non-party jurisdiction, could be extradited. Extradition of a bank clerk could occur if and when such a person traveled to the jurisdiction of an APUNCAC State Party.

Extradition of a front man could occur regardless because a false certification of beneficial ownership serves to aid and abet the serious crime of money laundering, satisfies the dual criminality requirement, and is, therefore, an extraditable offense under existing extradition treaties as well as UNTOC. UNTOC criminalizes the act of aiding, abetting, or facilitating the commission of a serious crime involving an organized criminal group.¹⁴⁷ Aiding and abetting is itself a crime, separate from a serious crime that is facilitated by this

¹⁴³ *Id.* art. 16(1) (“This article [regarding extradition] shall apply to the offences covered by this Convention. . . provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party”).

¹⁴⁴ For an international comparative analysis of dual criminality in international extradition law, see Blaas, Fey-Constanze, 2003, Double Criminality in International Extradition Law, LLM thesis, Stellenbosch, South Africa: University of Stellenbosch.

¹⁴⁵ *In re Nielsen* [1984] 2 WLR 737, 748–749.

¹⁴⁶ In the absence of an agreement, e.g., a status of forces agreement (SOFA).

¹⁴⁷ *Id.* art. 5(1)(b) (“Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally: Organizing, directing, aiding, abetting, facilitating or counselling the commission of serious crime involving an organized criminal group”).

offense. Significantly, UNTOC does not require that aiding and abetting meet the threshold for “serious crime”, involving a maximum punishment of four years imprisonment.¹⁴⁸ UNTOC does not require that aiding and abetting meet the threshold for a transnational crime. UNTOC criminalizes aiding and abetting serious crime involving an organized criminal group but does not define aiding, abetting, or facilitating the commission of a crime.¹⁴⁹

UNTOC makes each offense covered by the Convention, including aiding and abetting, “an extraditable offence in any extradition treaty existing between States Parties”.¹⁵⁰ Furthermore, “States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves”.¹⁵¹

Extradition could occur via either of two routes (Figures 9 and 10). An existing extradition treaty might permit extradition separately from UNTOC. Alternatively, the extradition provisions of UNTOC might be utilized. A prosecutor could choose the most suitable option. In certain cases, the first option may be suitable, while in other cases, the second option may be suitable. The existence of two options would minimize the chances that violations of the APUNCAC Rule would not be prosecuted. The presence of a credible threat of prosecution would deter violations of the Rule and, when violations occur, would provide a strong incentive for defendants to cooperate with prosecutors in exchange for probation or a reduced sentence.

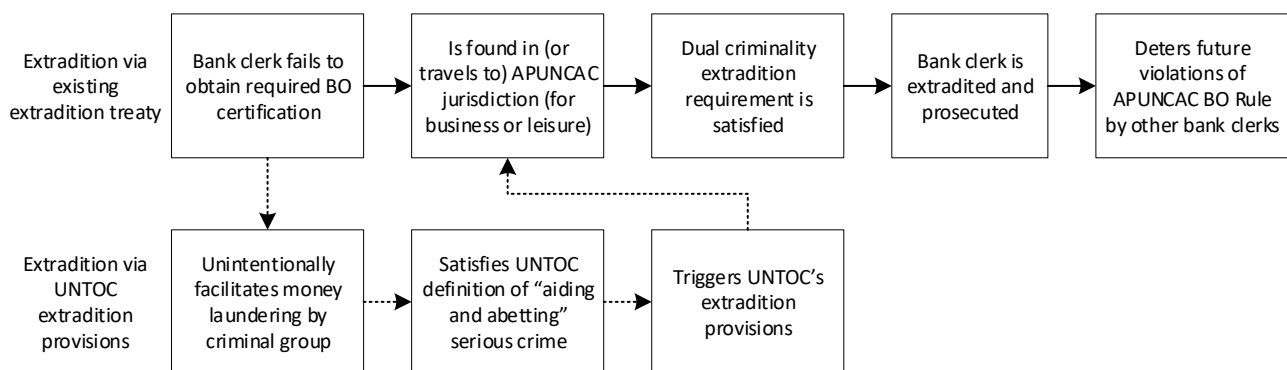


Figure 9. Two alternative routes for extraditing a bank clerk.

¹⁴⁸ Note that the text of Article 3(1)(b) focuses attention on serious crime where the offense is transnational in nature but includes a clause such that aiding and abetting is covered regardless of whether it meets the definition of a serious crime or a transnational crime (“This Convention shall apply, *except as otherwise stated herein*, to the prevention, investigation and prosecution of serious crime as defined in article 2 of this Convention; where the offence is transnational in nature and involves an organized criminal group”) (emphasis added). Article 5(1)(b) indicates that UNTOC applies to the offense of *aiding and abetting serious crime* regardless of whether aiding and abetting is classified as a serious crime or a transnational crime. Article 16(1) states that UNTOC’s extradition provisions apply to any offence covered by UNTOC (“This article [regarding extradition] shall apply to the offences covered by this Convention. . .”). Together, these provisions imply that UNTOC’s extradition provisions apply to the offense of aiding and abetting serious crime regardless of whether it meets the definition of a serious crime or a transnational crime. In principle, UNTOC may be used, together with existing extradition treaties, to extradite an accused person who is charged with the offense of aiding and abetting a serious crime.

¹⁴⁹ *Id.* art. 2.

¹⁵⁰ *Id.* art. 16(3).

¹⁵¹ *Id.* art. 16(6).

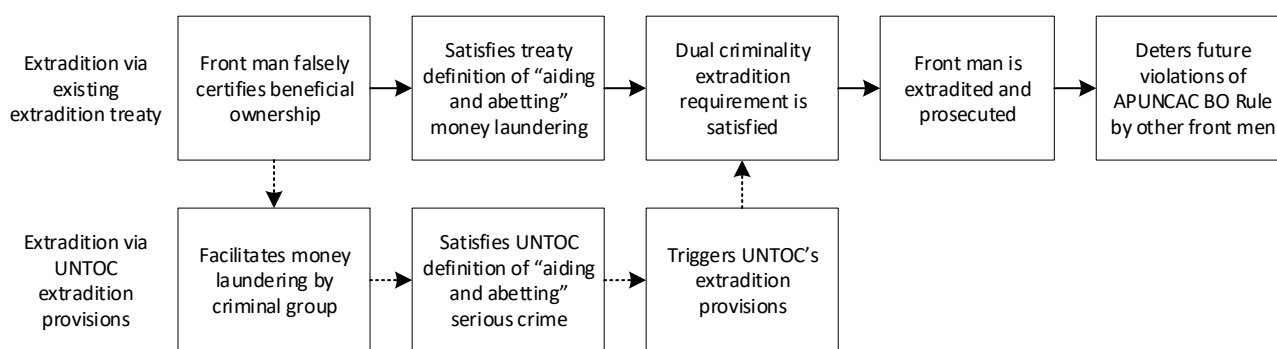


Figure 10. Two alternative routes for extraditing a front man.

UNTOC’s language was specifically crafted to encompass enablers and facilitators of money laundering. As noted above in Section 3.24, UNTOC obligates States Parties to implement requirements for customer identification and record-keeping to detect and deter money laundering, i.e., exactly the type of requirement represented by the APUNCAC Rule.¹⁵²

UNTOC obligates States Parties to sanction the crime of aiding and abetting serious crime.¹⁵³ Furthermore, Article 11 states:

Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences covered by this Convention are exercised to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.¹⁵⁴

This language, together with the previously cited UNTOC language, implies that States Parties should interpret discretionary aspects of domestic law in a way that facilitates extradition for violations of the APUNCAC Beneficial Owner Rule.

If a bank clerk in an offshore jurisdiction failed to observe the APUNCAC Rule by failing to submit the required beneficial owner certifications, or if a front man in an offshore jurisdiction falsely certified beneficial ownership, either offense would meet the UNTOC definition of a serious offense of a transnational nature because either offense is punishable by a maximum term of imprisonment of five years, and because either offense facilitates money laundering, a serious offense that has substantial transnational effects. These offenses make money laundering easier. UNTOC makes aiding or abetting serious crime an extraditable offense. A bank clerk or front man who aids, abets, or facilitates the commission of a serious crime such as money laundering may be extradited.¹⁵⁵

The APUNCAC Rule would be written into the criminal code, and would govern behavior, in each State Party to the Rule. Violations of the Rule would have the effect of aiding and abetting money laundering. A violation of the Rule would evince the constituent elements of the offense of aiding and abetting money laundering. A violation of the Rule would be an offense under the criminal code of the requested, as well as the requesting state, assuming that both are States Parties to the Rule. Having satisfied the dual criminality requirement, extradition could be obtained via existing extradition treaties or the extradition provisions of UNTOC.

To illustrate, the U.S. Department of Justice’s Antitrust Division has successfully applied the extraterritorial provisions of U.S. antitrust law to threaten overseas executives, accused of violating U.S. laws, with extradition and has secured the surrender of some

¹⁵² UNTOC art. 7(1)(a).

¹⁵³ *Id.* art. 11(1).

¹⁵⁴ *Id.* art. 11(2).

¹⁵⁵ “Aiding and abetting” would satisfy UNTOC’s extradition provisions regardless of how is treated in domestic law.

thirty or more overseas executives by offering them a deal in the form of a substantially reduced jail term (Joshua et al. 2008, p. 361; Krotoski 2015, p. 2; Mark 2018, p. 100). “Foreign defendants from Canada, France, Germany, Sweden, Switzerland, the Netherlands, Norway, United Kingdom, Korea, and Japan have served or are now serving prison terms in the United States for violating U.S. antitrust laws” (Joshua et al. 2008, p. 361). Those defendants would not have surrendered to U.S. authorities if they thought the risk of extradition was low.

In sum, U.S. antitrust law was applied to overseas executives operating outside the United States. The threat of extradition, trial, and imprisonment was genuine and was sufficient to compel the cooperation and surrender of overseas individuals accused of criminal acts.

Similarly, the APUNCAC Beneficial Owner Rule would be applied to bank clerks and front men operating outside the territory of APUNCAC States Parties. In response to the threat of extradition, trial, and imprisonment, overseas bank clerks and front men may find agreements to cooperate attractive, permitting prosecutors to target the criminal masterminds behind the schemes.

3.25.3. False Statements Risk Extradition

Many nations, including the U.S., have laws criminalizing a conspiracy, involving an agreement between two or more persons, to make false statements that impede, obstruct, or interfere with legitimate government functions (U.S. Department of Justice 2020a). This type of offense is a serious crime. In the U.S., the crime is punishable by a maximum term of imprisonment of five years.¹⁵⁶ In cases where this type of offense is criminalized in the requested and requesting states, satisfaction of dual criminality would permit extradition from the requested state to the requesting state, regardless of whether the states are APUNCAC States Parties.

A conviction may be obtained if a government proves that “the defendant knew the statements were false or fraudulent when made” (U.S. Department of Justice 2020a). A government “is not required to prove the statements ultimately resulted in any actual loss to the government of any property or funds, only that the defendant’s activities impeded or interfered with legitimate governmental functions” (U.S. Department of Justice 2020a).¹⁵⁷

A prosecutor who managed to obtain text messages directing a front man to send or receive funds could, in principle, demonstrate a conspiracy to make false statements that impede, obstruct, or interfere with legitimate government functions. The text messages would be evidence of an arrangement between two persons where the front man agreed to falsely certify beneficial ownership, where the principal and front man knew that the certification would be false. The front man would risk extradition under existing extradition treaties, including extradition via UNTOC’s extradition provisions. This risk of extradition would exist regardless of whether the requested and requesting states are APUNCAC States Parties.

A front man would have a choice: negotiate a cooperation agreement and provide evidence via deposition and testimony that implicates each person involved in the conspiracy or face imprisonment. If a front man chose to cooperate rather than face imprisonment, his testimony plus the text messages would be sufficient to demonstrate the existence of a conspiracy. A prosecutor would utilize this evidence to interrogate, pressure, and negotiate cooperation agreements with persons involved in the conspiracy. In this way, the prosecutor would obtain the evidence needed to convict anyone involved in the conspiracy who refused to cooperate.

¹⁵⁶ 18 USC § 371.

¹⁵⁷ See *United States v. Puerto*, 730 F.2d 627 (11th Cir.), cert. denied, 469 U.S. 847 (1984); *United States v. Tuohey*, 867 F.2d 534 (9th Cir. 1989); *United States v. Sprecher*, 783 F. Supp. 133, 156 (S.D.N.Y. 1992) (“[I]t is sufficient that the defendant engaged in acts that interfered with or obstructed a lawful governmental function by deceit, craft, trickery or by means that were dishonest”), modified on other grounds, 988 F.2d 318 (2d Cir. 1993).

3.25.4. Extradite or Prosecute

The problem of competence over transnational criminal fugitives may be stated as follows: “X is in State A. X carries out activities harmful to State B. Which state should prosecute?” Public international law recognizes two possible options:

- (a) the establishment of jurisdiction by State B followed by extradition of X from State A to State B; or
- (b) the refusal or failure of State A to extradite followed by the establishment of jurisdiction over X and prosecution by State A.

Increasingly, public international law incorporates the principle *aut dedere aut judicare*—meaning that a custodial state where an accused is found has an obligation to either extradite or prosecute. “The obligation to extradite or prosecute is imposed on the custodial state in whose territory an alleged offender is present” (Plachta 1999, p. 359). The custodial state has an obligation to take action to ensure that such individual is prosecuted either by another state, which indicates its willingness to prosecute by requesting extradition, or by the custodial state’s own national authorities (Plachta 1999, p. 359). The custodial state is in a unique position, by virtue of the presence of the alleged offender in its territory, to ensure that the accused does not escape justice (see Plachta 1999, p. 359).

The custodial state has an obligation to take the necessary and reasonable steps to apprehend an alleged offender and to ensure the prosecution and trial of such an individual by a competent jurisdiction. The custodial state has a choice between two alternative courses of action, both of which are intended to result in the prosecution of the alleged offender. The custodial state may fulfil its obligation by granting a request for the extradition of an alleged offender made by any other state, or by prosecuting that individual in its national courts. (Plachta 1999, p. 359)

Whether to surrender the person sought, or to pursue prosecution in the requested jurisdiction, would depend on factors including the competence and effectiveness of the relevant courts, potential legal obstacles, and feasibility of proceeding to trial.

“Such a stipulation appears in almost all conventions aimed at defining international offences as well as securing international cooperation in the suppression of such acts” (Plachta 1999, p. 334). For example, Article 7 of the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft states:

The Contracting Party in the territory of which the alleged offender is found shall, if it does not extradite him, be obliged, without exception whatsoever and whether or not the offense was committed in its territory, to submit the case to its competent authorities for the purpose of prosecution. Those authorities shall take their decision in the same manner as in the case of any ordinary offense of a serious nature under the law of the that state.¹⁵⁸

This mechanism for the implementation of the rule *aut dedere aut judicare* has been replicated in several subsequent conventions for the suppression of international offenses concluded under the auspices of the United Nations or its specialized agencies.¹⁵⁹ Article 9 of the Draft Code of Crimes against the Peace and Security of Mankind, titled “Obligation to extradite or prosecute”, adopted in 1996 by the International Law Commission at its 48th session and submitted to the UN General Assembly, stated: “the State Party in the territory

¹⁵⁸ Convention for the Suppression of Unlawful Seizure of Aircraft art. 7, December 16, 1970, 860 UNTS 105.

¹⁵⁹ Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971, 974 UNTS 177 (the Montreal Convention); Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, 1973, 1035 UNTS 167 (the New York Convention); International Convention Against the Taking of Hostages, 1979, 18 ILM 1456 (1979).

of which an individual alleged to have committed a crime set out in articles 17, 18, 19 or 20 is found shall extradite or prosecute that individual".¹⁶⁰

Bilateral and multilateral extradition treaties have incorporated the *aut dedere aut judicare* principle (Plachta 1999, p. 334). Modern extradition treaties typically include a provision that makes prosecution mandatory when extradition is denied on grounds of nationality (see Nadelmann 1990, p. 70). These provisions reflect "a developing sense of comity among governments in dealing with criminal violations of other governments' laws" (Nadelmann 1990, p. 42). For example, the European Convention on Extradition enshrines *aut dedere aut judicare* in article 6:

If the requested Party does not extradite its national, it shall at the request of the requesting Party submit the case to its competent authorities in order that proceedings may be taken if they are considered appropriate.¹⁶¹

The United Nations Model Treaty on Extradition incorporated a similar clause.¹⁶² Perhaps the most comprehensive and advanced formula was incorporated in the 1981 Inter-American Convention on Extradition. Article 2, which should be interpreted as imposing an obligation on the requested state to undertake the appropriate *judicare* action in every case where extradition is denied, states:

The requested State may deny extradition when it is competent, according to its own legislation, to prosecute the person whose extradition is sought for the offence on which the request is based. If it denies extradition for this reason, the requested State shall submit the case to its competent authorities and inform the requesting state of the result.¹⁶³

In sum, "the validity of the system based on *aut dedere aut judicare* has been confirmed not only in numerous international instruments, but also in domestic jurisprudence" (Plachta 1999, p. 334). A contemporary legal analysis concluded:

[P]ublic international law dictates that States have the legal obligation to either extradite or prosecute (*aut dedere aut judicare*) persons who commit serious international crimes. This obligation is predicated on the extraterritorial nature of international crimes and reflects an attempt of the international community to ensure that perpetrators are prosecuted either by the national authorities of that State or by another State which indicates that it is willing to prosecute the case by requesting extradition. (UNODC 2019)

Significantly, this principle is incorporated into UNTOC Article 16:

A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that he or she is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decision and conduct their proceedings in the same manner as in the case of any other offence of a grave nature under the domestic law of that State Party. The States Parties concerned shall cooperate with each other,

¹⁶⁰ Report of the International Law Commission on the work of its 48th session, UNGA Official Records, 51st session (A/51/10), 14. See also Timothy L. H. McCormack and Gerry J. Simpson, "The International Law Commission's Draft Code of Crimes against the Peace and Security of Mankind: An Appraisal of the Substantive Provisions", *Criminal Law Forum* 5: 1–55, (1994), p. 1.

¹⁶¹ European Convention on Extradition art. 6(2), opened for signature December 13, 1957, ETS No. 24. See also Explanatory Report on the European Convention on Extradition, Council of Europe 1969 at 17.

¹⁶² United Nations Model Treaty on Extradition, GA Res. 45/116, UN Doc. A/Res/45/116 (1991).

¹⁶³ Inter-American Convention on Extradition art. 2, opened for signature 25 February 1981 OAS Treaty Series No. 60 (entered into force 28 March 1992). Signatories are: Antigua and Barbuda, Argentina, Bolivia, Chile, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Nicaragua, Panama, Paraguay, St. Lucia, Uruguay, and Venezuela.

in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.¹⁶⁴

As a consequence of the expansion of extraterritorial jurisdiction, criminals are not likely “to escape punishment for their crimes merely by avoiding the state whose laws they have violated” (Nadelmann 1990, p. 42). The provisions of UNTOC, as well as existing multilateral legal assistance treaties, provide a framework for a requesting state party to effectively make use of a requested state party’s police forces in enforcing the laws and regulations of the requesting state party.

Recall that all but six minor jurisdictions are State Parties to UNTOC. Thus, a reasonable supposition is that State A is a State Party to UNTOC and is legally bound by the terms of UNTOC, including the Article 16 requirement to extradite or prosecute. Significantly, 116 of 196 nations are parties to the Vienna Convention on the Law of Treaties (UN 2023).¹⁶⁵ Thus, a reasonable supposition is that State A is also a party to the Vienna Convention and is legally bound by the terms of the convention. Article 27, titled “Internal law and observance of treaties”, states: “A party may not invoke the provisions of its internal law as justification for its failure to perform a treaty”. If State A is a party to the Vienna Convention, it may not invoke a conflict with domestic law as a justification for failure to perform its obligations under UNTOC, including Article 16. The legal obligation to either extradite or prosecute implies that a recalcitrant bank clerk or front man would face a genuine risk of prosecution for violations of the APUNCAC Rule if State A is a party to the APUNCAC Rule. A bank clerk or front man in a recalcitrant jurisdiction (perhaps BVI, the Caymans, Malta, or Cyprus) who traveled to State A would risk extradition to State B or prosecution by State A because State A would, under UNTOC, be obligated to either extradite, or prosecute violations of the APUNCAC Rule. A violator who traveled to State A would be held accountable for violations of the APUNCAC Rule.

3.25.5. Willingness to Prosecute

Assume that State A is a party to the APUNCAC Rule. State A cannot fulfill its UNTOC Article 16 obligation to either extradite or prosecute (*aut dedere aut judicare*) by “electing” to prosecute X and then saying that it is unwilling or unable to prosecute. Election of the option to prosecute X implies that State A is willing and able to prosecute. If State A is unwilling or, for any reason, unable to prosecute, it could not fulfill its UNTOC Article 16 obligation by “electing” to prosecute. If State A’s laws, regulations, or criminal procedures are incompatible with the prosecution of X, State A cannot prosecute X and cannot elect the option of prosecuting X. State A could only fulfill its UNTOC Article 16 obligation by extraditing X. There would be no other option if State A chooses to fulfill its obligations as an UNTOC State Party.

However, if State A laws, regulations, and criminal procedures enable prosecution of X, and assuming that State A is a party to UNTOC, why might State A willingly prosecute X—who might be a State A national—for violations of the APUNCAC Beneficial Owner Rule? A strong advantage of choosing to prosecute is that State A could assert that it is in full compliance with its UNTOC and FATF AML obligations while avoiding extradition of State A’s national to face trial in a foreign jurisdiction, i.e., the courts of the requesting state. State A nationals might be expected to support this policy to avoid prosecution via a foreign court and foreign procedures that may lack the protections and safeguards offered by State A’s criminal justice system.

In sum, there is reason to think that State A may be willing to prosecute X. X would reasonably fear prosecution by State A or extradition and prosecution in State B courts. A prosecutor (in either State A or State B) would be able to offer X an attractive plea bargain: an agreement to cooperate and provide information about criminals using X to hide beneficial ownership in exchange for deferred prosecution and a recommended

¹⁶⁴ UNTOC art. 16(10).

¹⁶⁵ Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, 1155 UNTS 331.

sentence of probation. The alternative would be to risk prosecution, trial, and imprisonment. Via a plea bargain, the prosecutor—and State B—would have achieved the objective of securing X’s cooperation in prosecuting the criminals orchestrating the criminal activity. State A would have satisfied its UNTOC Article 16 obligations. A plea bargain would avoid the time, expense, effort, and optics of prosecuting a State A national. All parties would benefit from a plea bargain.

3.25.6. Serial Extradition

Suppose that a fugitive bank clerk “X” is in State A, but State A is not an APUNCAC State Party. Fugitive X is wanted by State B (an APUNCAC State Party) for violations of the APUNCAC Beneficial Owner Rule. If State A has not adopted the Rule, dual criminality is not satisfied. Neither UNTOC nor the London Scheme may be used to extradite X directly from State A to State B.

However, it may be possible to obtain the extradition of X from State A to State M, followed by extradition from State M to State B (Figure 11).¹⁶⁶ In principle, State B might obtain the agreement of State M to request extradition of X from State A to State M. If both State M and State B have adopted the Rule, dual criminality is satisfied. State B could then request the extradition of X from State M to State B via UNTOC or the London Scheme, achieving the objective of extradition of X from State A to State B.

The CARICOM Arrest Warrant Treaty (AWT), for example, would permit the extradition of X from one Caribbean Community jurisdiction (i.e., State A) to another Caribbean Community jurisdiction (i.e., State M) (see analysis above).

Suppose that State M is the Bahamas and has adopted the Rule. Thus, dual criminality is satisfied for the extradition of X from State M to State B. The London Scheme would permit the extradition of X from the Bahamas to any of 56 Commonwealth Nations, including Botswana, Cameroon, Ghana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Sierra Leone, South Africa, Swaziland, Tanzania, Uganda, and Zambia (Peters and Peters n.d.). In sum, it would be possible, via serial extradition, to achieve the objective of extraditing X from State A, which is not an APUNCAC State Party and has not adopted the Rule, to numerous African countries that have been victimized by criminals who have used the international financial system to launder the illicit proceeds of their crimes. The use of serial extradition would greatly expand the dragnet that could be employed to capture and prosecute recalcitrant violators of the APUNCAC Rule.

Serial extradition would depend on the willingness of State M to cooperate with State B’s request for the extradition of X from State A to State M, followed by extradition from State M to State B. The assumption, however, is that States M and B are States Parties to the APUNCAC Rule, which is written in a way that captures individuals who interact with a “national of a State Party” to the Rule, or “an entity within the jurisdiction of a State Party” to the Rule. The Rule lumps all States Parties together and captures individuals and entities who interact with any national of any State Party and any entity within the jurisdiction of any State Party.

The APUNCAC Rule is a regulation that would be communally enforced by the entire community of APUNCAC States Parties, in the same way that EU regulations are communally enforced by the entire community of EU member states.¹⁶⁷ The expectation is

¹⁶⁶ In *Bozano v. France* [1986] 9 EHRR 297, the applicant was convicted *in absentia* in Italy of serious crimes. Following his arrest in France, the Italian authorities sought his extradition. The French court refused to extradite him on the basis that French law did not allow extradition following a conviction *in absentia*. However, the French authorities deported him to Switzerland, and the Swiss extradited him to Italy. There was no apparent irregularity in the extradition process between Switzerland and Italy. Provided there has been no collusion between the trial State and the State of refuge, this method of returning a fugitive offender does not offend provisions under the 1957 European Convention on Extradition.

¹⁶⁷ Adoption of an EU regulation is equivalent to each EU member state adopting the regulation individually. It is analogous to adoption of the APUNCAC Rule by a set of individual States Parties. Enforcement necessarily involves a prosecutor from one State Party pursuing prosecution of the accused. In either case, it involves cooperation and mutual legal assistance among the applicable police and criminal justice systems. In the EU, authorities may utilize the European Arrest Warrant Treaty to obtain custody of the accused. An APUNCAC

that State M would cooperate with State B's request to extradite X from State A to State M, followed by extradition from State M to State B, because both State M and State B are APUNCAC States Parties that have agreed to adopt and enforce the APUNCAC Rule across all APUNCAC States Parties. In the same way, each EU member state cooperates with all other EU member states in enforcing EU regulations across the EU, including (for example) the criminal enforcement of EU antitrust regulations. Each EU member state is obliged to cooperate with a request by another EU member state that is seeking the extradition of a fugitive violator of EU regulations. Each EU member state is obligated to cooperate with other EU member states to ensure that fugitive violators do not escape prosecution. In the same way, enforcement of the APUNCAC Rule would rest on the mutual obligation of APUNCAC States Parties to cooperate with extradition requests.¹⁶⁸

Serial extradition would need to conform to the principle of specialty, which is codified in numerous bilateral extradition treaties and regional extradition schemes as well as the CARICOM AWT.¹⁶⁹ Specialty is a requirement that an extradited person shall not be proceeded against, sentenced, detained, re-extradited to a third State, or subjected to any other restriction of personal liberty in the territory of the requesting State for any offense committed before surrender other than the offense for which extradition was granted or any other offense in respect of which the requested State consents (Bilalli-Zendeli 2019, p. 41; UNODC 2019). Specialty serves as a safeguard against prosecutions in the requesting State for political offenses and violations of other substantive rules of extradition law, such as dual criminality and the principle of *ne bis in idem* (UNODC 2019). Certain extradition treaties, including the CARICOM AWT and the European Arrest Warrant Framework Decision (EAW FD), permit the specialty provision to be waived by the executing State (Mackarel and Nash 1997, p. 956; Tinsley 2021, p. 28).¹⁷⁰

Regardless, the violation of the APUNCAC Rule that would constitute the basis for extradition from State A to State M would involve the same underlying facts and constituent elements that would constitute the basis for extradition from State M to State B.¹⁷¹ The principle of specialty would not be violated. The conditions for serial extradition would be satisfied.

State Party prosecutor would utilize UNTOC extradition provisions and existing extradition treaties to obtain custody of the accused.

¹⁶⁸ In theory, an accused person might be pursued by multiple states, creating conflicts. Currently, however, there is a dearth of prosecution. Regardless, states may resolve jurisdictional conflicts via deference to the state with the greatest interest in exercising jurisdiction, according to the principle of comity.

¹⁶⁹ CARICOM AWT art. 11 "Rule of Specialty" ["A requested person who has been surrendered pursuant to Article X shall not be prosecuted or sentenced for an offence committed prior to his surrender other than that for which he was surrendered unless: (a) he consents to such prosecution or sentence; (b) he is being prosecuted or sentenced for a lesser offence disclosed by the facts upon which the request for surrender had been made; (c) the executing judicial authority consents to his being so dealt with for another applicable offence; or (d) the requested person having had an opportunity to leave the territory of the Participating Member to which he has been surrendered has not done so within forty-five (45) days of his final discharge, or has returned to that territory after leaving it".]

¹⁷⁰ *Id.* art. 11; Council Framework Decision 2002/584/JHA on the European arrest warrant, art. 27(1), O.J. L 190 [hereinafter EAW FD].

¹⁷¹ The French Court of Cassation has interpreted an 'offence... other than that for which he was extradited' as prohibiting prosecution for new (alleged) facts distinct from those in respect of which extradition was sought (Tinsley 2021, p. 28). Tinsley, Alex, 2021, "Specialty: Arresting an Elusive 'Right' in European Extradition Law", *New Journal of European Criminal Law* 12: 23–35. The Court of Justice of the European Union (CJEU) adopted a nearly identical position, focusing on the degree of correspondence of the 'constituent elements' for which a person was surrendered (Tinsley 2021, p. 29). The U.S. Ninth Circuit Court adopted the same position, focusing on whether "the essential character of the acts criminalized is the same", not whether the elements of the offense are identical or whether the scope of the liability is coextensive/same. *United States v. Knotek*, 925 F.3d 1118, 1131–32 (9th Cir. 2019).

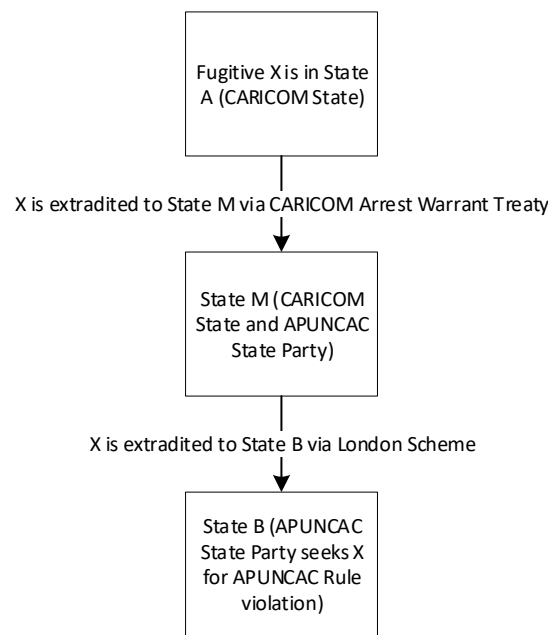


Figure 11. Extradition of X from State A to State B via State M for violation of the Rule.

3.25.7. Reciprocity

The U.S., the UK, and the Organisation for Economic Co-operation and Development (OECD) Member States are leaders in the fight against terrorism and combating the financing of terrorism. In principle, the Rule potentially offers—unlike any other strategy—a practical means of exerting a degree of extraterritorial control over recalcitrant offshore enablers and facilitators of money laundering who indirectly enable and facilitate the financing of terrorism. A State Party that actively complies with extradition requests related to the application of the Rule might expect reciprocity from like-minded States that are equally concerned about terrorism and the financing of terrorism. If the OECD Member States agree that the application of the Rule offers a promising strategy to combat the financing of terrorism, extradition is an essential element of an effective deterrent, and reciprocity is key to the effectiveness of the strategy, one might expect that OECD Member States would support reciprocity and would support requests to extradite individuals who enable the type of money laundering that facilitates terrorism.

3.25.8. A Genuine Threat

UNTOC “has become an important legal basis for extradition, where there is no legal extradition treaty between countries” (Zanotti 2006, p. viii). “UNTOC has removed differences among national legal systems” that were barriers to international judicial assistance (Zanotti 2006, p. viii). States Parties to UNTOC are obliged to adopt domestic laws and practices that facilitate extradition regarding the crimes covered by UNTOC. While implementation has been uneven, UNTOC has been utilized in numerous cases as the legal basis for extradition (Schloenhardt 2021, pp. 7–11). In key cases, UNTOC has been utilized as the sole legal basis for extradition between States that have no bilateral treaties and are not parties to another extradition agreement (Schloenhardt 2021, pp. 10–11). Extradition is a genuine threat.

In sum, the APUNCAC Rule, in combination with UNTOC, would pose a genuine risk of extradition and imprisonment for a recalcitrant bank clerk or front man. Violations of the APUNCAC Rule would qualify as serious, extraditable offenses under UNTOC.

A suspect could potentially be extradited for *aiding or abetting* a serious crime or *conspiracy to commit* a serious crime. If a prosecutor managed to obtain text messages directing a front man to send or receive funds, in violation of the APUNCAC Rule, and obtained the cooperation of the front man to testify regarding the plan, this would be

evidence of a conspiracy to make false statements that impede, obstruct, or interfere with legitimate government functions. It would be evidence of a conspiracy to hide the true beneficial owner, violate AML regulations, and engage in money laundering. A bank clerk who willfully failed to obtain the required beneficial owner certifications and (inadvertently or otherwise) served to aid and abet money laundering could be extradited for the offense of aiding and abetting money laundering.

A bank clerk or front man who violated the APUNCAC Rule would be vulnerable to extradition and prosecution. The prosecutor's objective would be to use this leverage to pressure the accused individuals into cooperation agreements where they would agree to provide evidence and testimony that implicate the principals directing and controlling the criminal scheme.

It should not be a surprise that UNTOC offers a solid basis for extradition for violations of the APUNCAC Rule. Both UNTOC and the Rule are designed to fight money laundering. They are specifically crafted to address this crime and associated crimes. UNTOC is specifically designed to enable and facilitate the extradition of suspects who engage in money laundering, conspire to engage in money laundering, or aid and abet money laundering.

3.25.9. Aiding and Abetting

Application to international crimes of the offense of *aiding and abetting* a serious crime "has never been called into question" (Ventura 2019, p. 183). "Aiding and abetting requires acts or omissions that assist, encourage or lend moral support to crimes" (*actus reus*) (Ventura 2019, p. 176). "The accused must have acted or omitted to act with knowledge that his/her acts or omissions assist the commission of the crime in question" (*mens rea*) (Ventura 2019, p. 177). "An aider and abettor does not control the commission of a crime but merely provides assistance to those who do" (Ventura 2019, p. 179).

Significantly, "aiding and abetting liability can be incurred on the basis of omissions as well as actions" (Ventura 2019, p. 182). "Aiding and abetting by omission requires the accused to have a legal duty to act in the circumstances" (Ventura 2019, p. 188). "In aiding and abetting by omission cases, the *actus reus* is satisfied if the crimes would have been substantially less likely had the accused acted pursuant to his legal duty to act" (Ventura 2019, p. 189).

A conviction for aiding and abetting money laundering does not require that the aider and abettor share a common plan or intent to launder illicit funds. "Aiding and abetting does not require the existence of a common plan; the latter is irrelevant for an aiding and abetting conviction. . . a single individual can aid and abet crimes committed by the principals" (Ventura 2019, p. 178). "An aider and abettor need not share an agreement with anyone" (Ventura 2019, p. 181). "No evidence of a plan or agreement between the aider and abettor and the principal perpetrator is required" (Ventura 2019, p. 187). An aider and abettor "need not share the intent of the principals" (Ventura 2019, p. 179). "The principals need not even know of the aider and abettor's existence or contribution to the crime" (Ventura 2019, p. 182).

Furthermore, "the *actus reus* need not be specifically directed to practically assist, encourage or lend moral support to the commission of crimes" (Ventura 2019, p. 185). "It is unnecessary to show that each given act individually constituted substantial assistance in order to satisfy the *actus reus*; it may involve multiple acts that cumulatively substantially contribute to the crime" (Ventura 2019, p. 186).

Importantly, "the location of where the *actus reus* takes place can be remote from the time and location of where the crime in question is committed; the accused need not have been personally present during the commission of the crime" (Ventura 2019, p. 185).

It is not necessary to prove that the accused exercised independent initiative: "the aider and abettor need not possess a certain level of authority or power or have an ability to exercise independent initiative in order to make a substantial contribution to the crimes" (Ventura 2019, p. 187). Furthermore, "it is not necessary to establish that the aider and abettor's contribution served as a precondition to the crime or that the crime would not

have occurred but for the aider and abettor's contribution (i.e., that the contribution was a *sine qua non*)" (Ventura 2019, p. 187). In addition, "the principal perpetrator need not have been identified, tried or convicted" (Ventura 2019, p. 188). Moreover, "the assistance need not be given directly to the principal perpetrator and used by him in the commission of the crime; the essential question is whether the accused's acts and conduct can be said to have contributed substantially to the commission of the crime" (Ventura 2019, p. 188).

Significantly, UNTOC criminalizes "conspiracy to commit [and] attempts to commit" all of the offenses established by the Convention.¹⁷² When conspiracy or attempt has been criminalized, international law does not require the crime in question to be fully completed or committed before aiding and abetting liability is triggered (see Ventura 2019, p. 228). "It is enough that the crime be attempted" (Ventura 2019, p. 228). This lowers the bar that triggers aiding and abetting liability. A prosecutor who manages to obtain text messages directing a front man to send or receive funds could, in principle, demonstrate a violation of the APUNCAC Rule and demonstrate a conspiracy to make false statements that impede, obstruct, or interfere with legitimate government functions and demonstrate a conspiracy to commit money laundering.

The person accused of aiding and abetting a crime "need not know the precise crime which was intended and which was committed by the principal, but he must be aware of its essential elements, including the state of mind of the principal" (Ventura 2019, p. 189). A front man would, of course, be aware of the state of mind of a person directing him. A bank clerk would be aware of the state of mind of criminals intent on laundering illicit funds to the extent that the bank had conducted the type of standard anti-money laundering awareness, education, and training required by banking regulators.

In cases where the aider and abettor's conduct may have facilitated the commission of multiple crimes, it is sufficient for a prosecutor to demonstrate that the aider and abettor was aware, or had knowledge, "that one of a number of crimes would probably be committed and one of those crimes was in fact committed" (Ventura 2019, p. 189). This condition would be satisfied to the extent that a bank clerk was implicated via the testimony of a front man who had been caught receiving directions to send or receive funds, was guilty of a violation of the APUNCAC Rule, and testified that the bank clerk aided and abetted the front man's actions by cooperating to violate the APUNCAC Rule.

Significantly, "the *actus reus* can occur before, during or after the crime in question is committed" (Ventura 2019, p. 185). This would permit prosecution for violations of the APUNCAC Rule that occurred after funds were laundered, for example, when criminals seek to withdraw laundered funds from offshore accounts. In cases of specific intent crimes such as money laundering, "the accused need only know or be aware of the principals' specific intent" to launder illicit funds (Ventura 2019, p. 189). "The accused need not share the intent of the principal perpetrator" (Ventura 2019, p. 190). A bank clerk who was aware, via the bank's AML training program, of the intent of criminals to launder illicit funds through financial institution accounts, yet knowingly violated the APUNCAC Rule, serving to aid and abet those criminals, would satisfy the *mens rea* for the crime of aiding and abetting money laundering. "The accused need not have acted, or omitted to act, for the purpose of assisting the commission of crimes" (Ventura 2019, p. 190).

The establishment of the APUNCAC Rule would establish a legal requirement to obtain certification, by the purported beneficial owner, when funds are transmitted in amounts exceeding USD 3000. A recalcitrant *bank clerk* who ignored that requirement after being informed of the requirement, and subsequently processed a fund transmission without obtaining the required certification, would be guilty of violating a legal requirement. This offense would satisfy the *actus reus* of the crime of aiding and abetting money laundering because the crime of money laundering would have been substantially less likely had the accused acted pursuant to his legal duty to act. This offense would satisfy the *mens rea* to the extent that the bank clerk had knowledge of the certification requirement

¹⁷² UNTOC art. 6(1)(b)(ii).

and knowingly did not obtain the required certification. While a bank clerk might plead ignorance regarding an initial violation, a notice of debarment for an initial violation would include a recitation of the Rule and a warning that violations of the Rule are subject to criminal penalties. A subsequent violation of the Rule would satisfy the *mens rea* requirement. A bank clerk could not plead ignorance.

A recalcitrant *front man* who violated the Rule would be guilty of violating a legal requirement. This offense would satisfy the *actus reus* of the crime of aiding and abetting money laundering because the crime of money laundering would have been substantially less likely had the accused acted pursuant to his legal duty to act. This offense would satisfy the *mens rea* because the APUNCAC certification procedure would require positive assent to a statement that the front man was the true beneficial owner of the funds in question. A front man could not say that he was unaware that he had falsely certified ownership.

This analysis suggests that violations of the APUNCAC Beneficial Owner Rule meet the definition of aiding and abetting the serious crime of money laundering and, therefore, are extraditable crimes under UNTOC. This implies that violations of the Rule would pose a genuine risk of extradition. It implies that prosecutors would possess the necessary leverage to pressure bank clerks and front men in offshore jurisdictions to cooperate, provide useful information, and unravel even the most complex money laundering and organized criminal schemes.

3.25.10. Conspiracy to Commit Money Laundering

Conspiracy consists of an agreement between two or more persons to commit an unlawful act. From a prosecutorial standpoint, conspiracy is easier to establish since it does not require completion of the underlying offense. Furthermore, “the government need not prove a formal agreement but can demonstrate its existence through circumstantial evidence or by inference from the defendants’ actions” (Sigler 2009, p. 593).

The defendant’s conscious participation in the conspiracy may be inferred from circumstantial evidence. The government need not prove the defendant knew all the details of, objectives of, or identity of all the other participants in the conspiracy. Besides acts included in the underlying substantive offense, other acts the defendant committed in furtherance of the objectives of the conspiracy are often sufficient to demonstrate defendant was a knowing participant. (Sigler 2009, pp. 597–98)

Elements

In the U.S., conspiracy to commit money laundering is a serious offense that carries a 20-year maximum sentence (Wydra 2004, p. 149).¹⁷³ The elements of a conspiracy to commit money laundering were defined in *Whitfield v. United States*, ultimately decided by the U.S. Supreme Court, when the district court instructed the jury, involving defendants indicted for conspiracy to commit money laundering, as follows:

In order for you to find any defendant guilty of this crime, you must be convinced that the Government has proven each of the following elements beyond a reasonable doubt: First, that two or more persons, in some way or manner, came to a mutual understanding to try to accomplish a common and unlawful plan, as charged in the indictment; and second, that the defendant under consideration knowingly and willfully became a member of such conspiracy. (Wydra 2004, p. 147)

The court charged the jury to decide, based upon the evidence presented, whether the government had proven the elements beyond a reasonable doubt. The defendants were convicted.

¹⁷³ Section 3.25.10 illustrates one of several paths a prosecutor might pursue to obtain extradition and prosecution. Discussion of variation in the treatment of conspiracy across international jurisdictions is beyond the scope of the present article.

The issue that arose, which was ultimately decided by the U.S. Supreme Court, was whether the commission of an overt act is a required element of the offense of conspiracy to commit money laundering. The Supreme Court unanimously decided that a conviction for conspiracy to commit money laundering did not require proof of an overt act in furtherance of the alleged conspiracy.¹⁷⁴ Thus, a federal prosecutor need not prove that an overt act occurred. Instead, a jury may decide, based upon the evidence presented, whether the defendant was a member of a group of two or more people who came to a mutual understanding to accomplish an unlawful plan as charged in the indictment.

Agreement

In criminal law, the offense of conspiracy requires an agreement to commit an unlawful act. An agreement in this context does not need to be explicit; instead, mutual agreement constituting a conspiracy may be inferred from the acts of the parties and any other circumstantial evidence indicating concert of action for the accomplishment of a common purpose.¹⁷⁵

An agreement between a principal and front man to violate the APUNCAC Rule would be evinced by a text message from the principal to the front man to send or receive funds, knowing that the APUNCAC Rule would require the front man to perform a certification of beneficial ownership that the principal and front man knew to be false, followed by an affirmative response by the front man. An affirmative response could be a text message, or actual transmission or receipt of funds as directed by the principal. Either act would complete the plan.

The clearest evidence of the illicit nature of the plan would be evidence that the front man falsely self-certified beneficial ownership, in combination with the text message from the principal directing the front man to send or receive funds. Having established the illicit nature of the plan and overt acts in furtherance of the plan, a prosecutor could demonstrate a conspiracy to impede, obstruct, or interfere with legitimate government functions as well as a conspiracy to hide the true beneficial owner and the origin and nature of the funds in question, presumably for the purpose of money laundering. A prosecutor could use this evidence to pressure the front man into a cooperation agreement where he would testify regarding the plan, testify against any person involved in the plan, and provide the evidence needed by the prosecutor to secure their cooperation and testimony regarding anyone involved in the plan. This tactic would be used by the prosecutor to unravel the criminal scheme.

Intent to Promote

Conviction for the offense of *conspiracy to commit money laundering* requires that a prosecutor prove that the defendant *conspired* “to conduct and attempt to conduct a financial transaction affecting interstate commerce, which transaction involved the proceeds of specified unlawful activity, (that is,) . . . with the intent to promote the carrying on of such specified unlawful activity” (U.S. Department of Justice 2020c).

The term *with the intent to promote the carrying on of specified unlawful activity* means that the defendant must have conducted or attempted to conduct the financial transaction for the purpose of promoting (that is, to make easier, facilitate or to help bring about) the carrying on of one of the crimes listed as specified crimes within the statute. By carrying on crime, it may be that the crime to be carried on is one that will be committed in the future. (U.S. Department of Justice 2020b)

¹⁷⁴ Whitfield v. United States, 543 US 209 (2005).

¹⁷⁵ See States v. Lopez-Medina, 461 F.3d 724, 750 (6th Cir. 2006) (stating that a plan may be inferred from defendant’s conduct); United States v. Weidner, 437 F.3d 1023, 1033 (10th Cir. 2006) (holding a conspiracy can be inferred from defendants’ conduct); United States v. Nelson, 383 F.3d 1227, 1229 (10th Cir. 2004) (finding that an agreement constituting a conspiracy may be inferred from the acts of the parties and any other circumstantial evidence indicating concert of action for the accomplishment of a common purpose).

“‘Promoting’ and ‘facilitating the promotion’ of unlawful activity is satisfied by proof that the defendant’s action made the unlawful activity easy or less difficult” (U.S. Department of Justice 2020b, FN1).¹⁷⁶ “It is not necessary to show that the defendant intended to commit the additional crime himself. The government need only show that in conducting the financial transaction, the defendant intended to make the unlawful activity easier or less difficult for someone to commit” (U.S. Department of Justice 2020b).¹⁷⁷

The financial transaction need not be linked to a specific future offense. The government is required to prove only that in conducting the financial transaction, the defendant intended to promote a specified illegal activity generally. For example, buying beepers or two-way radios for use in the drug business promotes specified unlawful activity because it makes future drug dealing, in general, less difficult.¹⁷⁸ (U.S. Department of Justice 2020b)

An elaborate conspiracy to hide the identity of the beneficial owner controlling a transaction would make financial transactions involving illicit funds “easy or less difficult”. It would be evidence of a conspiracy involving a plan to commit money laundering. It would satisfy the requirement that the prosecutor proves “intent to promote the carrying on of specified unlawful activity”, i.e., financial transactions involving illicit funds. The actions of a principal to direct and coordinate with, a front man to knowingly make a false certification of beneficial ownership in violation of the APUNCAC Beneficial Owner Rule would make it less difficult to conduct financial transactions involving illicit funds. These actions would qualify as a conspiracy to commit money laundering. Anyone involved in the conspiracy and anyone who aids and abets the conspiracy would qualify for extradition under existing extradition treaties as well as UNTOC. In combination with the APUNCAC Rule, existing extradition treaties, including the extradition provisions of UNTOC, would present a genuine risk of extradition to any bank clerk or front man in an offshore jurisdiction who chose to violate the APUNCAC Rule.

Application

A prosecutor who manages to obtain text messages directing a front man to send or receive funds would, in principle, demonstrate a violation of the APUNCAC Rule. The text messages would be overt acts in furtherance of an unlawful plan to violate the APUNCAC Rule, hide the beneficial owner controlling the transactions in question, and hide the true origin and nature of the funds in question, presumably for the purpose of laundering the funds and preventing authorities from tracing the funds to their true origin. The agreement of a front man to these directions, or the action of sending or receiving funds in response to these directions and knowingly performing certification of beneficial ownership that the principal and front man knew to be false, would complete the illicit plan and satisfy the requirement of a mutual understanding to accomplish an unlawful plan.

The *mens rea* of the unlawful nature of the plan would be established by the fact that the front man would, under the APUNCAC Rule, be required to perform a certification of beneficial ownership of the funds in question that he knew to be false. A front man could not deny that he had knowingly performed a false certification of beneficial ownership, and the person directing the front man could not deny that he had directed and controlled the actions of the front man in sending or receiving funds, as well as the performance of the certifications required to send or receive funds.

A front man would have a choice: negotiate a cooperation agreement to provide evidence via deposition and testimony that implicates persons involved in the conspiracy, or face imprisonment. If a front man chose to cooperate rather than face imprisonment,

¹⁷⁶ See, e.g., *United States v. Rogers*, 788 F.2d 1472, 1476 (11th Cir. 1986); *United States v. Jenkins*, 943 F.2d 167, (2d Cir. 1991).

¹⁷⁷ *United States v. Corona*, 885 F.2d 766, 773 (11th Cir. 1989) (the defendant himself does not have to be involved in the offense being facilitated).

¹⁷⁸ *United States v. Jackson*, 935 F.2d 832 (7th Cir. 1991).

this testimony, plus the text messages, would potentially demonstrate the existence of a conspiracy. A prosecutor would utilize this evidence to interrogate, pressure, and negotiate cooperation agreements with persons involved in the conspiracy. In this way, the prosecutor would obtain the evidence needed, including evidence of the illicit nature of the funds in question, to convict anyone involved in the conspiracy who refused to cooperate.

3.25.11. Significance

The significance of the APUNCAC Rule is that proving the *mens rea* of an unlawful plan to violate the APUNCAC Rule is simpler than proving the *mens rea* for the crime of money laundering. The latter requires that the prosecutor prove knowledge of the illicit nature of the funds in question, which is far more difficult than proving knowledge that a false certification of beneficial ownership, under the APUNCAC Rule, is unlawful. To prove knowledge of guilty intent under the APUNCAC Rule, a prosecutor could simply recite the Rule, the warning that false statements are punishable by penalties including imprisonment, the certification made by the front man in violation of the Rule, the evidence that the front man was directed by another person to send or receive funds, and the definition of a true beneficial owner, which is inconsistent with the possibility that some other person controlled or directed the true beneficial owner.

By definition, a true beneficial owner controls the transaction. The owner is not controlled by another person. The prosecutor would have proven that the front man was not the true beneficial owner and knew that he was involved in a plan to make a false certification of beneficial ownership. The testimony of a cooperating front man regarding the principal directing the front man would, together with the text messages directing the front man, be sufficient to demonstrate the principal's *mens rea* regarding the plan to violate the APUNCAC Rule. The front man would presumably testify that the principal controlled and directed a plan to have the front man perform a certification that both parties knew to be false.

An elaborate conspiracy to hide the identity of the beneficial owner controlling a transaction would potentially be evidence of a conspiracy to commit money laundering. A prosecutor could use this evidence to pressure anyone involved in the conspiracy to testify regarding the conspiracy. Anyone involved would have a choice: negotiate a cooperation agreement and provide evidence and testimony that implicates each person involved in the conspiracy, or face imprisonment. If low-level criminals chose to cooperate rather than face imprisonment, their testimony, together with evidence such as text messages, would be sufficient to demonstrate the existence of a conspiracy. A prosecutor would utilize this evidence to interrogate, pressure, and negotiate cooperation agreements with persons involved in the conspiracy. In this way, the prosecutor would obtain the evidence needed to convict anyone involved in the conspiracy who refused to cooperate.

A prosecutor could, in principle, prove the existence of a conspiracy to commit the crime of money laundering. Conspiracy is a serious crime. Having proven the existence of a conspiracy, the prosecutor could also prove that the actions of a recalcitrant bank clerk who failed to obtain the required APUNCAC certifications served to aid and abet a serious crime. The prosecutor could prove that the actions of a front man in serving as a front man who falsely certified beneficial ownership aided and abetted a serious crime. Therefore, the prosecutor could prove that the bank clerk and front man were guilty of the crime of aiding and abetting a serious crime. This would qualify the bank clerk and front man for extradition under UNTOC, since UNTOC provides for extradition for all crimes covered by UNTOC, and since the crime of aiding and abetting a serious crime is a crime covered by UNTOC. In addition, the front man would be guilty of conspiracy and eligible for extradition under UNTOC for conspiracy.

The significance is that each bank clerk and front man would, at the outset, be aware of the risk that violations of the APUNCAC Rule could expose them to a genuine risk of extradition, trial, and imprisonment. The deterrent effect, as well as pressure to cooperate with prosecutors, would be strong. The combination of the APUNCAC Rule and UNTOC

would create a genuine risk of punishment for offshore enablers and facilitators of money laundering who are currently beyond the reach of prosecutors.

3.26. INTERPOL Red Notice

The enforcement process would typically begin when a jurisdiction submits a request for an INTERPOL Red Notice. A Red Notice is a potent tool for combating financial crime (Estlund 2018). A Red Notice seeks the arrest or provisional arrest of wanted persons for the purpose of extradition (Estlund 2018). A Red Notice allows financial crime criminal suspects and witnesses to be detained for purposes of extradition (Estlund 2018). With a single exception, every country in the world is a participating member of INTERPOL (INTERPOL 2023). Each member country maintains a National Central Bureau (NCB) that acts as a liaison with INTERPOL. A Red Notice is enforced when local officials, e.g., immigration officials, check the passenger manifest of an incoming flight at an airport against the INTERPOL database, find a match, and provisionally arrest or detain a suspect for the purpose of extradition (Estlund 2018). “Once a Notice is circulated to INTERPOL’s member countries, the information is available to law enforcement and other government personnel at all points of entry and exit. This alerts officials to the movement and location of the subject” (Estlund 2018). The implementation of a Red Notice immobilizes suspects in any country to which they travel (Estlund 2018).

“A Notice may also be published on INTERPOL’s website” and on lists of high-risk suspects provided to financial institutions by law enforcement agencies (Estlund 2018). A Red Notice inhibits the ability of a subject to travel freely, maintain his or her livelihood, or conduct financial transactions (Estlund 2018). Subjects may be unable to establish a relationship at reputable financial institutions (Estlund 2018). The consequences are significant.

3.27. Enforcement in Practice

The enforcement process may be clarified through an example. Consider the following hypothetical scenario:

Kenya becomes a party to the model protocol. The governments of all 196 countries in the world are notified of the protocol and the provisions requiring bank clerks to record beneficial ownership information with regard to currency, check, and money order deposits and wire transfers involving Kenyan nationals, entities or funds. Each government notifies its domestic bank and non-bank financial institutions. However, a bank clerk in the British Virgin Islands (BVI) fails to observe the recordation requirement and is debarred. The debarment process includes official notification of debarment and recitation of the recordation requirement. The same bank clerk subsequently handles a \$10 million bank wire involving a Kenyan government minister to a BVI corporate account, but again fails to observe the recordation requirement. Kenya files a request with BVI for arrest and extradition under the terms of UNTOC for aiding and abetting concealment of the identity of the person who owns the \$10 million.

At this point, BVI authorities must make a decision about whether or not to comply with the request. The decision would hinge on whether, in the view of BVI authorities, the bank clerk’s failure to observe the recordation requirement was proper or improper. If BVI authorities determine that the failure was improper and served to aid and abet the concealment of the identity of the person who owns the \$10 million, then extradition would presumably be approved. However, if BVI authorities determine that the failure was not improper, it is unlikely that extradition would be approved.

If BVI authorities approve extradition, a precedent would be set. Consistent application of the law dictates that similar cases be treated in the same way, implying that BVI would be forced to make a decision about whether to incorporate the

recordation requirement into its domestic regulatory regime and whether to extradite in cases where bank clerks fail to observe the recordation requirement. The model protocol would, in essence, force jurisdictions around the world to decide whether or not to incorporate the recordation requirement into their domestic regulatory regimes.

Each jurisdiction would make an independent determination about the benefits and costs of incorporating the recordation requirement into its domestic regulatory regime. If the presumed benefits exceed the presumed costs, a jurisdiction would presumably move to incorporate the recordation requirement into its domestic regulatory regime. If the presumed costs exceed the presumed benefits, a jurisdiction would presumably reject the recordation requirement and any request for extradition based on that requirement.

However, the United States, the UK, and the OECD countries are aggressive leaders in the fight against money laundering because money laundering permits terrorists to hide large amounts of monies that are used to fund terrorism. The recordation requirement would permit investigators to pull back the veil that currently hides the identities of persons who use anonymous corporate vehicles in BVI, the Caymans, and Panama for illicit purposes. The recordation requirement would penetrate the anonymity that currently protects terrorists and criminals by protecting their financial assets. If major OECD countries begin incorporating the recordation requirement into their domestic regulatory regimes, it would become a *de facto* world standard for any nation that is serious about fighting money laundering. It would become a litmus test for any nation that claims to fight money laundering.

Panama is a party to UNTOC. If the recordation requirement becomes a *de facto* world standard, if Panama is judged on the basis of whether it conforms to world standards in the fight against money laundering, and if foreign investment in Panama depends on whether Panama conforms to world standards in the fight against money laundering, Panamanian leaders may feel that it is in their best interests to incorporate the recordation requirement into their domestic regulatory regime and cooperate with extradition requests when bank clerks handle large multi-million dollar bank wires but fail to observe the recordation requirement. If Panamanian leaders choose to reject the recordation requirement and reject extradition requests when bank clerks handle large multi-million dollar bank wires but fail to observe the recordation requirement, they would not be able to say that they are in compliance with world standards regarding regulations to fight money laundering. If Panama is unable to shake its reputation as a jurisdiction where money laundering and criminal activity are rife, foreign investors will be wary of investing in Panama.

Panama might choose to formally adopt the recordation requirement and incorporate the requirement into its domestic regulatory regime, then fail to cooperate with extradition requests. Formal adoption of the requirement would give Panamanian leaders the cover to say that Panama conforms to world standards in the fight against money laundering. However, this tactic would not protect Panamanian nationals who travel abroad.

Panama is a party to UNTOC and is bound by the terms of UNTOC. Consequently, the act of aiding, abetting, and facilitating the concealment of the identity of persons who acquire illicit funds is a crime under the domestic laws of all UNTOC parties, including Panama. Panama might fail to cooperate with extradition requests, but it would not be in a legal position to protect any of its nationals who travel to another UNTOC party jurisdiction and are arrested for aiding, abetting, and facilitating the concealment of the identity of, for example, a Kenyan government minister who transmits \$10 million to a Panamanian bank account.

If a previously debarred Panamanian bank clerk handled the transmission of \$10 million from a Kenyan government minister into a Panamanian bank account but failed to observe the recordation requirement and subsequently traveled to a jurisdiction outside of Panama, the clerk would, under the model protocol, be at-risk of arrest and imprisonment for aiding, abetting, and facilitating concealment of the minister's ownership of the \$10 million. Significantly, 190 nations are parties to UNTOC and are legally bound by the terms of UNTOC, including the terms whereby any party can request extradition of a suspect from the jurisdiction of another party (United Nations 2023). The only United Nations Member States that are not parties are Bhutan, Papua New Guinea, the Solomon Islands, Somalia, South Sudan, and Tuvalu. This implies that a Panamanian bank clerk who handled the transmission of \$10 million from a Kenyan government minister into a Panamanian bank account but failed to observe the recordation requirement and subsequently traveled to a jurisdiction outside of Panama would be at-risk of arrest and imprisonment whenever he or she traveled outside of Panama because Kenya could request extradition if the clerk traveled to the territory of any of the 190 nations that are parties to UNTOC.

While there may be bank clerks who are content to spend their entire lives within Panama, the risk of traveling to other jurisdictions for business or leisure would be a significant cost of failing to observe the recordation requirement. Many bank clerks would resist employment at a financial institution whose practices and policies are inconsistent with the recordation requirement and place clerks at-risk of arrest and imprisonment whenever they travel abroad.

As a consequence, the model protocol would create a powerful mechanism for controlling money laundering in distant offshore locations that is currently absent from all other existing and proposed strategies for controlling corruption and impunity. Ratification and implementation of the model protocol would fall within the power of potential States Parties. States Parties would not need to wait for distant offshore jurisdictions to implement reforms. States Parties would apply the provisions of the model protocol requiring documentation of the beneficial owner and source of funds transmitted by bank wire, and would apply UNTOC to extradite individuals who violate this rule in distant offshore locations such as the British Virgin Islands, the Cayman Islands, or Panama. This suggests why the model protocol would likely be more effective than the strategy of implementing a global registry of companies, which would require the cooperation of offshore locations such as the British Virgin Islands, the Cayman Islands, and Panama. (Yeh 2020a, pp. 155–57)

This example clarifies how extraterritorial jurisdiction would be enforced. Travel outside the territory of a recalcitrant jurisdiction would be risky. "Many foreign governments possess the statutory authority to deliver noncitizens to a requesting government even in the absence of a treaty" (Nadelmann 1990, p. 72). Once a suspect has been apprehended, extradition would depend upon a determination by the relevant jurisdiction that the requested, as well as the requesting, state is a State Party to both APUNCAC and UNTOC, and obligations as a State Party compel extradition.

The accused would presumably fight extradition. Extradition would depend on a determination that requirements for extradition under the relevant extradition treaty are satisfied and extradition is consistent with international obligations as a State Party to UNTOC, the obligation to enforce requirements for customer identification and record-keeping intended to deter and detect money laundering, and the obligation to extradite individuals who violate those requirements. If a majority of OECD Member States agree to implement and enforce the APUNCAC Rule, consistent with UNTOC customer identification AML requirements, the risk of arrest and extradition would be genuine, and the deterrent effect would be significant.

In principle, extradition would pose a genuine risk to violators of the Rule. In New Zealand, for example, an extraditable offense is an offense that satisfies one of three conditions: (a). an offense punishable under the law of an extradition country with a minimum penalty of 12 months imprisonment, (b). an offense punishable under New Zealand law with a similar sentence term, or (c). an offense on the list of extraditable offenses of a relevant extradition treaty (Parnell Law Chambers 2021). The first condition would be met because violations of the APUNCAC Rule may be penalized by a sentence of five years imprisonment. The existence of an extradition treaty is not a requirement of extradition. Thus, the requirements for extradition would be satisfied in New Zealand. The requirements in other OECD Member States are not dissimilar, implying that extradition would be a genuine risk whenever a suspect traveled to an OECD Member State.

3.28. Objective Territorial Principle

What legal principle would permit an APUNCAC State Party to exercise governmental authority beyond its territorial borders? The ‘objective territorial principle’ is the basis for the ‘effects principle,’ which in turn is the basis for extraterritorial assertion of the APUNCAC Beneficial Owner Rule. International law permits a state to apply criminal law if a person caused a criminal result in the state (“objective territoriality”) (Gallant 2022, p. 555).

According to Gallant, prevention of harm to persons, property, and interests within the state is “the dominant international law-based justification for objective territorial jurisdiction” (Gallant 2022, p. 215). “Authority to prevent harmful events from occurring on a state’s territory is central to the sovereignty of the state” (Gallant 2022, p. 215). “The great majority of states exercise authority to prohibit acts outside the state which cause criminal results within the state” (Gallant 2022, p. 215). Furthermore, “most states today apply this theory in their law of criminal jurisdiction, to one extent or another” (Gallant 2022, p. 268). “It appears broadly in civil law, common law, Islamic law, and other Asian law states” (Gallant 2022, p. 268). “Objective territoriality is accepted by all or almost all states under international law and implemented by most of them” (Gallant 2022, p. 269).

According to Gallant, “a state has authority to legislate concerning events occurring on its territory” (Gallant 2022, p. 557). “Specifically, it has authority to criminalize acts elsewhere which cause ill results on its territory, where the required results are elements of the crime” (Gallant 2022, p. 557). “States have authority to criminalize acts outside their territory intended to cause criminal results on their territory or are objectively likely to cause criminal results there, even if the criminal scheme is interrupted before completion or, for some other reason, the results do not occur on their territory” (Gallant 2022, p. 557).

“States have authority to apply law both to actors on their territory and to events on their territory caused by actors outside” the territory (Gallant 2022, p. 558). “Modern practice allows a state to criminalize acts of secondary participants outside the state” (Gallant 2022, p. 558). “This includes those who, under the law of the state to which the crime is localized, were not principals, but who were accomplices, conspirators, or otherwise participated in the crime” (Gallant 2022, p. 558). Furthermore, “a preparatory crime (such as conspiracy or attempt) aimed at commission of a substantive crime in a target state may be criminalized by that state, even if no criminal result occurs there” (Gallant 2022, pp. 557–58).

Significantly, “international law allows localization of entire crimes to any place where a single element occurs by act or result” (Gallant 2022, p. 558). “A state may apply its criminal law to all those who participate in acts which are elements of a crime, where at least one of the acts was committed on its territory or a criminal result occurred on its territory” (Gallant 2022, p. 558). “Additionally, a state may apply its law to supporting acts of accessories, accomplices, and co-conspirators, wherever those acts occurred” (Gallant 2022, p. 559). “It may ‘localize’ the entire crime and supporting acts to itself, so that its courts may apply its own laws to them” (Gallant 2022, p. 559).

According to Gallant, “the authority of a state to criminalize direct and foreseeable harms on its territory remains established in practice and *opinio juris*” (Gallant 2022,

p. 569).¹⁷⁹ Other states may enter objections. A state may consider those objections. Regardless, “the enactment of a statute is almost always an expression of *opinio juris* that the statute is within the legal authority of the state” (Gallant 2022, pp. 585–86). “Decisions under these statutes are often expressions of *opinio juris* under international law as well” (Gallant 2022, p. 586).

In sum, via the principle of objective territoriality, international law permits a state to apply criminal law if a person caused a direct, foreseeable, criminal result within the state. According to the principle of objective territoriality, a State Party to the APUNCAC Beneficial Owner Rule may apply the Rule, and criminal penalties for violating the Rule, if violations cause a direct, foreseeable criminal result within the State Party. The Rule regulates the conduct of distant offshore banking personnel. The Rule requires banking personnel to record beneficial ownership information in the FINCEN database. A failure to record such information would serve to aid and abet the crime of money laundering within the State Party. Aiding and abetting is itself a serious crime, separate from the crime of money laundering. The omission of a duty required by law, i.e., required by the APUNCAC Rule, to obtain and submit beneficial ownership information, would serve to aid and abet money laundering within the State Party. This meets the definition of a crime, according to the principle of objective territoriality, where the criminal result occurs within the State Party. Thus, according to international law, the State Party has criminal jurisdiction over the person who caused that result. The objective territorial principle provides the legal basis for application of the Rule, and penalties for violations of the Rule, to distant offshore banking personnel.

3.29. Effects Principle

According to Gallant, “the fact that a criminal result (elemental effect) occurs in a state in most cases ends any controversy about whether a claim of objective territorial jurisdiction over the crime is acceptable under international law” (Gallant 2022, pp. 275–76). Increasingly, however, a state may assert jurisdiction over offenses occurring outside its territory but having non-elemental effects within its territory. This assertion of jurisdiction, based on the ‘effects’ principle, is accepted by the U.S., the EU, China, India, Japan, and Israel (Gallant 2022, p. 272). Assertion of jurisdiction based on the effects principle may also be inferred in jurisdictions that have criminalized cartel-related offenses, including Australia, Brazil, Canada, Iceland, Indonesia, Israel, Japan, South Korea, Norway, Russia, Thailand, the U.S., Zambia, and a majority of EU member states (Shaffer et al. 2015, p. 312); Mexico and the United Kingdom (Mark 2018, p. 97); Colombia, Chile, and Peru (Gutiérrez 2023, p. 506); Cambodia, Laos, Myanmar, Philippines, and Vietnam (Burgess 2023, p. 470); Saudi Arabia, South Africa, and New Zealand (DLA Piper 2022, p. 8); Malaysia and Taiwan (Jones Day 2012).¹⁸⁰ “This acceptance by some of the world’s largest trading powers

¹⁷⁹ In customary international law, *opinio juris* is the second element necessary to establish a legally binding custom. *Opinio juris* denotes a subjective obligation, a sense on behalf of a state that it is bound to the law in question. The International Court of Justice reflects this standard in ICJ Statute, Article 38(1)(b) by reflecting that the custom to be applied must be “accepted as law”.

¹⁸⁰ Cartels involve domestic effects of conduct that may take place wholly or in part outside the regulating territory; this activity has the ‘object or effect’ of restricting competition and would be difficult to prosecute without application of the effects principle. Application of the effects principle to extraterritorial conduct is documented in Section 3.30 regarding Japan, South Korea, China, Vietnam, Taiwan, Australia, Russia, Brazil, Argentina, Kenya, Nigeria, South Africa, the U.S., and EU. These jurisdictions apply their domestic laws in ways that capture extraterritorial conduct by foreign nationals outside the regulating territory if that conduct has the object or effect of restricting competition within the territory of the regulating state. The ‘object or effect’ language is codified, for example, in Article 101(1) of the Treaty on the Functioning of the European Union (TFEU). Nishioka (2020, p. 599) (“In the EU, Article 101(1) of the TFEU prohibits concerted practices or agreements that have the ‘object or effect’ of restricting competition”). Article 2(2) of the Swiss Cartel Act (SCA) explicitly provides that “[t]his Act applies to practices that have an effect in Switzerland, even if they originate in another country”. An English translation provided by the federal council is available at <https://www.admin.ch/opc/en/classified-compilation/19950278/index.html> accessed 22 September 2023. In law and practice, criminalization of cartel-related offenses involves application of the effects principle. “The SCA explicitly adopts the effects doctrine” (Nishioka 2020, p. 600). The Swiss Federal Administrative Court ruled that “the effects principle is intended to be leveraged to apply the cartel law even in cases

indicates that some version of effects jurisdiction is acceptable in public international law” (Gallant 2022, p. 272). “It is said that ‘virtually all jurisdictions apply some form on an effects test’” (Nishioka 2020, p. 591). It is “widely accepted that the application of competition law based on effects in a state’s territory does not contravene public international law” (Nishioka 2020, p. 593). In sum, the jurisdiction of a state may extend to extraterritorial conduct by individuals who are not nationals of the state if that conduct has an effect within state territory (Janis 2003, p. 322).

International acceptance of the effects principle is driven by rapid advances in technology, in combination with the merging of product, service, and financial markets across borders, which has accelerated globalization. A consequence of globalization is that “actions carried out in one place often produce effects in many different and sometimes very distant places” (Battini 2011, p. 76). Extraterritorial actions by foreign actors produce domestic effects. In response, domestic officials legislate extraterritorial regulations that seek to control behavior by foreign actors that has internal domestic effects. “[T]he increasing extraterritoriality of domestic regulation, either de jure or de facto, is an unavoidable effect of globalization” (Battini 2011, p. 62). “[T]he interdependence between States is making extraterritoriality increasingly unexceptional” (Battini 2011, p. 62).

Extraterritorial regulation, however, creates conflicts. Extraterritorial regulation by State A, when applied to nationals of State B in the territory of State B, potentially conflicts with the laws of State B. How have courts dealt with this conflict?

Judicial decisions regarding antitrust regulation have clarified how this conflict may be resolved. Conflict in the field of antitrust arose because domestic regulations sought to regulate foreign, as well as domestic, actors. Regulation of foreign actors is justified because, in global markets, “the anti-competitive activities of producers or service providers can affect consumers in every country in which their goods are sold or their services are provided” (Battini 2011, p. 63).

3.29.1. United States

According to Joelson, “it is now settled law that the [U.S.] Sherman [Antitrust] Act was intended to apply even to acts of foreign persons in their own countries in certain circumstances” (Joelson 2017, p. 44). “The nationality of the wrongdoers is not important, nor is the locale of the damaging activity”, as long as there is a demonstrable, or foreseeable, domestic effect (Joelson 2017, p. 46).

The pivotal U.S. case involving the effects principle is *United States v. Aluminum Co. of America*.¹⁸¹ A Canadian firm participated in a cartel based in Switzerland that restricted imports to the United States. A U.S. federal court held that since the companies in the cartel had affected U.S. commerce by restricting imports to the U.S., the Canadian firm’s activities were properly within the regulatory purview and legislative jurisdiction of the United States.¹⁸² The court found that extraterritorial application of U.S. law to the Canadian firm was justified because “any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders”.¹⁸³ Subsequently, the Second Restatement of the Foreign Relations Law of the United States declared:

in which the infringement of competition law was committed abroad”. BVGer, 19 December 2013—Gaba, 2013/4 RPW 760, s 3.3.14.1. The Swiss Federal Supreme Court “concluded that its approach based on an effects test was not contrary to the limitation of public international law” (Nishioka 2020, p. 601). While regulatory frameworks differ across countries, what “the countries all have in common” “when they define the international or geographical scope of their competition law” is a focus on “whether conduct violates relevant legal provisions”—i.e., whether the conduct in question has a domestic anticompetitive effect. See Nishioka (2020, p. 602). If there is a domestic effect, anticompetitive conduct is illegal, regardless of the geographical location of the actors. Criminalization of cartel-related offenses implies endorsement, acceptance, and application of the effects principle.

¹⁸¹ *United States v. Aluminum Co. of America*, 148 F.2d 416, 442–48 (2d Cir. 1945).

¹⁸² *Id.*

¹⁸³ *Id.* at 443.

A state has jurisdiction to prescribe a rule of law attaching legal consequences to conduct that occurs outside its territory and causes an effect within its territory, if. . . (i) the conduct and its effect are constituent elements of activity to which the rule applies; (ii) the effect within the territory is substantial; (iii) it occurs as a direct and foreseeable result of the conduct outside the territory; and (iv) the rule is not inconsistent with the principles of justice generally recognized by states.¹⁸⁴

The Third Restatement of the Foreign Relations Law of the United States reaffirmed the effects principle, declaring that a state has jurisdiction with respect to “conduct outside its territory that has or is intended to have substantial effect within its territory”.¹⁸⁵

In 1993, the U.S. Supreme Court upheld the effects principle in *Hartford*.¹⁸⁶ The facts in *Hartford* illustrate the need for extraterritorial regulation. Four major U.S. primary insurers decided to promote an industry-wide change from “occurrence-based” to “claims-made” insurance policies (Battini 2011, p. 62). Their efforts were successful. British reinsurers agreed to reinsure American primary insurers only for claims-made policy forms. The effect was to reduce the total amount of claims paid to U.S. policy holders. In the *Hartford* case, the conduct of British reinsurers had a direct, negative impact on U.S. policy holders. The Attorneys General for several states and many private plaintiffs brought antitrust suits against American and British insurance companies, including the British reinsurers, alleging that their conduct amounted to an illegal conspiracy under the Sherman Antitrust Act (Battini 2011, p. 63).

In its 1993 decision, the U.S. Supreme Court held that U.S. antitrust rules are applicable to the conduct of British reinsurers doing business in London, beyond U.S. borders, because it is “well established by now that the Sherman Act applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States”.¹⁸⁷ “According to Justice Souter, international comity considerations could prevent the exercise of U.S. jurisdiction only when there was a ‘true conflict’ between U.S. and foreign law” (Battini 2011, p. 64). “But a true conflict does not exist ‘where a person subject to regulations by two states can comply with the laws of both.’”¹⁸⁸ “Therefore, since the British reinsurers did not argue that British law required them to act in violation of U.S. law, there was no reason to decline jurisdiction” (Battini 2011, p. 64).

In 2016, the U.S. Supreme Court reaffirmed the effects principle as a basis for asserting extraterritorial jurisdiction.¹⁸⁹ The court held that the American RICO law applies to both foreign and domestic enterprises regarding predicate offenses such as money laundering that the U.S. Congress intended to apply to extraterritorial behavior if a RICO enterprise affects commerce directly involving the United States.¹⁹⁰

3.29.2. European Union

While the EU lagged in adopting the effects principle, it is now judicially accepted and codified in law and practice. “In the EU, Article 101(1) of the [Treaty on the Functioning of the European Union (TFEU)] prohibits concerted practices or agreements that have the

¹⁸⁴ American Law Institute, *Restatement (Second) of the Foreign Relations Law of the United States* §17 (1965).

¹⁸⁵ American Law Institute, *Restatement (Third) of the Foreign Relations Law of the United States* §402(1)(c) (1987).

¹⁸⁶ *Hartford Fire Insurance Co v. California*, 509 US 764 (1993). In 2010, the U.S. Supreme Court, in *Morrison v. National Australia Bank*, applied a strict presumption against extraterritoriality when the ‘focus’ of the relevant statute occurred outside the territory of the United States (Rotman 2021, p. 49). Rotman, Edgardo, 2021, “Extraterritorial Application of United States Law”, in *Regulating Fraud across Borders: Internationalised Criminal Law Protection of Capital Markets*, edited by Edgardo Rotman, Oxford, UK: Hart, pp. 41–72. This reversed 40 years of federal court decisions and threatened to upend *Hartford*. However, the U.S. Congress quickly passed legislation clarifying its intent, reversing *Morrison*, and restoring the ‘conduct’ and ‘effects’ tests that existed prior to *Morrison* (Rotman 2021, p. 51). Congress intended to sanction willful conduct that poses a social threat to the vital values and interests of the American people, including conduct that occurs extraterritorially outside U.S. borders (Rotman 2021, pp. 66–67).

¹⁸⁷ *Hartford Fire Insurance Co. v. California* at 796.

¹⁸⁸ *Id.* at 799.

¹⁸⁹ *RJR Nabisco, Inc. v. European Cmty*, 136 S. Ct. 2090, 2102, 2104, 2105 (2016).

¹⁹⁰ *Id.*

‘object or effect’ of restricting competition” (Nishioka 2020, p. 599). The European Commission first affirmed the extraterritoriality principle in 1977, stating that the Commission “can act against restrictions of competition whose effects are felt within the territory under [its] jurisdiction, even if companies involved are locating and doing business outside the territory, and of foreign nationality, have no link with that territory, and are acting under an agreement governed by foreign law” (Bertrand and Ivaldi 2006, pp. 8–9).

This approach was later embraced in 1988 by the European Court of Justice (ECJ) in the *Wood Pulp* case.¹⁹¹ “The ECJ was asked to determine whether Article 81 of the EC Treaty should apply to U.S., Canadian, Swedish and Finnish producers conspiring to fix wood pulp prices in the EU” (Battini 2011, p. 65). “Defendants claimed that the EU lacked jurisdiction over them, since they were not incorporated in the EU” (Battini 2011, p. 65). “Furthermore, as one of the U.S. defendants was involved in an export cartel legally authorized in the United States, they also claimed that application of the EU law would actually violate the international public law duty of non-interference” (Battini 2011, p. 65).

“The ECJ rejected both claims, using arguments very similar to those used by the U.S. Supreme Court in *Hartford*” (Battini 2011, p. 65). The ECJ reasoned that EU laws were applicable because “the producers implemented their pricing agreements within the common market”, therefore, “what matters is not the place where the agreement or the decision is taken but where it is implemented, i.e., where products are sold” (Bertrand and Ivaldi 2006, p. 9). “An official from the Antitrust Division of the U.S. Department of Justice noted that the European Union’s ‘implementation doctrine’ is very close to, if not indistinguishable from the American ‘effects test’” (Batz 2007, p. 82).

The ECJ rejected the assertion that the extraterritorial application of the EU law was contrary to public international law regarding the principle of non-interference: “There is not, in this case, any contradiction between the conduct required by the United States and that required by the Community”.¹⁹² The ECJ ruled that “the Commission’s decision is not contrary to Article 85 of the Treaty or to the rules of public international law relied on by the applicants”.¹⁹³

In 2017, in its long-anticipated *Intel* decision, the ECJ unambiguously embraced the effects test, serving to align EU competition rules with U.S. law (Prete 2018, p. 492).¹⁹⁴ The ECJ ruled that conduct outside the EU that has anticompetitive effects within the EU market triggers the application of EU competition rules.¹⁹⁵ The ruling established that it is not necessary to meet an implementation test. Satisfaction of an effects test would be sufficient to establish jurisdiction.

3.29.3. Significance

The significance of the preceding analysis is that the international community accepts the effects principle. International acceptance of the effects principle implies that the legal foundation for the APUNCAC Rule is internationally accepted. This is seen most clearly in antitrust law.

“Both the United States and the EU apply their respective antitrust laws extraterritorially to anti-competitive conduct taking place outside their borders, but producing effects, or being implemented, within them” (Battini 2011, p. 65). Extraterritorial conduct “causing territorial anticompetitive economic effects is the basis for prosecution” (Gallant 2022, p. 283). “Both the United States and the European Union accept that direct, substantial, intended effects on their territories caused by outside anticompetitive agreements are actionable domestically” (Gallant 2022, p. 284).

¹⁹¹ ECJ, Joined Cases 89, 104, 114, 116, 117 and 125 to 129/85, *A. Ahlström Osakeyhtiö and others v. Commission*, ECR 1988, at 5193.

¹⁹² ECJ, ECR 1988, at 5244.

¹⁹³ *Id.*

¹⁹⁴ Case C-413/14 P, *Intel v Commission*, EU:C:2017:632.

¹⁹⁵ *Id.*, paras. 40–47.

The effects principle has been affirmed by U.S. federal courts, the U.S. Supreme Court, and the European Court of Justice (ECJ). The Permanent Court of International Justice (PCIJ) endorsed the effects principle:

[T]he courts of many countries, even of countries which have given their criminal legislation a strictly territorial character, interpret criminal law in the sense that offences, the authors of which at the moment of commission are in the territory of another State, are nevertheless to be regarded as having been committed in the national territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there. . . [T]he Court does not know of any cases in which governments have protested against the fact that the criminal law of some country contained a rule to this effect.¹⁹⁶

The PCIJ found that ordinary international law has no rule prohibiting a nation's exercise of extraterritorial jurisdiction (see [Janis 2003](#), p. 31).¹⁹⁷

This form of de jure extraterritorial regulation is now an accepted feature of international law. International law permits a state to exercise its jurisdiction to promulgate rules, whether it be legislation or administrative decrees, prohibiting conduct elsewhere from having an "effect" within the State ([Knott 2010](#), p. 158). Criminal codes from countries adopting civil law, common law, Islamic law, and Asian law systems apply the effects principle ([Gallant 2022](#), p. 310). The extraterritorial regulation of behavior is judicially accepted if there is no contradiction between the conduct required by the regulating state and the conduct required by the state where a defendant may be found.

The major international anticorruption treaties either permit or require a degree of extraterritorial jurisdiction ([Ireland-Piper 2012](#), p. 140).¹⁹⁸ "International treaties that either permit or require the exercise of extraterritoriality are indicative of an increased reliance on non-territorial grounds of jurisdiction" ([Ireland-Piper 2012](#), p. 140). Treaty-based assertions reflect international consensus among parties and provide an element of certainty and consistency across jurisdictions ([Ireland-Piper 2012](#), pp. 140–41).

UNTOC permits a State Party to assert jurisdiction, according to the effects principle, over the crime of aiding, abetting, facilitating or counselling the commission of serious crime involving an organized criminal group "committed outside its territory with a view to the commission of a serious crime within its territory".¹⁹⁹ The States Parties to UNTOC, including all but six minor jurisdictions worldwide, have agreed that the effects principle is a proper basis for asserting extraterritorial enforcement jurisdiction.

The international judicial acceptance of extraterritorial regulation based on the effects principle is affirmed by the rapid expansion of such regulation by the U.S. and EU (see Section 3.31, below). As a practical matter, these regulations could not have been implemented and given extraterritorial effect in the absence of judicial acceptance by foreign jurisdictions. If there is no conflict with internal legal requirements in those foreign jurisdictions, and if a regulation seeks to control conduct having a direct, substantial, and foreseeable effect on the regulating state or is necessary to guard against regulatory evasion, extraterritorial regulation based on the effects principle is internationally accepted.

Judicial acceptance of this principle implies that the extraterritorial behavioral requirements dictated by the APUNCAC Rule are internationally legal if the behavior required by the APUNCAC Rule is not inconsistent with the conduct required by the state where a

¹⁹⁶ *SS Lotus (France v Turkey)*, PCIJ, Ser A, No 10 (1927) 23.

¹⁹⁷ *Id.* at 16–32.

¹⁹⁸ See, e.g., Convention on Combating the Bribery of Foreign Public Officials in International Business Transactions, *opened for signature* 17 December 1997, [1999] ATS 21 (entered into force 15 February 1999); United Nations Convention against Corruption, *opened for signature* 31 October 2003, 2349 UNTS 41 (entered into force 14 December 2005); Inter-American Convention against Corruption, Organization of American States, *opened for signature* 29 March 1996, [2000] CTS 21 (entered into force 6 March 1997); Criminal Law Convention on Corruption, *opened for signature* 27 January 1999, ETS No 173 (entered into force 1 July 2002); Additional Protocol to the Criminal Law Convention on Corruption, *opened for signature* 15 May 2003, ETS No 191 (entered into force 1 February 2005).

¹⁹⁹ UNTOC art. 15(2)(c)(i).

bank clerk or front man may be found. Since there are no laws prohibiting a bank clerk from reporting beneficial owner information when required to do so, and there are no laws requiring a front man to make false declarations regarding beneficial ownership, there is no inconsistency between the conduct required by the APUNCAC Rule and the conduct required by any state where a bank clerk or front man may be found.²⁰⁰ This implies that the APUNCAC Rule is not inconsistent with internationally accepted practice regarding extraterritorial regulation of conduct, behavior, and actions. In short, implementation of the APUNCAC Rule, by any state, would not be inconsistent with internationally accepted norms and practices.

According to the effects principle, States Parties to the APUNCAC Beneficial Owner Rule may regulate the conduct of distant offshore banking personnel for the purpose of fighting the effects of money laundering that are experienced within the territory of States Parties. The APUNCAC Rule requires banking personnel to record beneficial ownership information in the FINCEN database. A failure to record such information would have the effect of facilitating the crime of money laundering, a crime that has substantial effects within the territory of States Parties to the Rule. The effects principle provides the legal basis for the application of the Rule to distant offshore banking personnel.

The APUNCAC Rule would debar distant offshore banking personnel who do not comply with the recordation requirements. A precedent for this approach is the U.S. practice of sanctioning foreign nationals who do not reside or conduct business within the territory of the U.S. but whose conduct has effects within the territory of the U.S.; for example, individuals whose conduct serves to aid and abet terrorists.²⁰¹ The Rule seeks to isolate recalcitrant offshore banking personnel by debarring any national of a State Party who conducts financial transactions with the assistance of a debarred person, and by debarring any individual who transmits funds originating from the territory of a State Party with the assistance of a debarred person.²⁰² Repeat offenses are punishable by criminal penalties.²⁰³ If debarred individuals in high-risk jurisdictions transmit or retransmit funds that originate from the territory of a State Party to a foreign destination, they are subject to criminal penalties.²⁰⁴ The application of criminal penalties to individuals who cooperate with debarred individuals is analogous to the U.S. practice of enforcing criminal penalties against individuals who violate U.S. sanctions by continuing to do business with persons on the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) list of Specially Designated Nationals and Blocked Persons (SDN list) ([U.S. Department of the Treasury 2023](#)).²⁰⁵ In both cases, criminal penalties are enforced against individuals who do not cooperate in isolating the sanctioned persons.

While any state could unilaterally adopt the APUNCAC Rule, extradition and prosecution of violators would depend upon satisfaction of existing requirements for extradition. In cases where dual criminality is required to obtain extradition of a bank clerk, extradition could only be obtained if the requested state, in addition to the requesting state, had adopted the APUNCAC Rule. In those cases, the APUNCAC Rule would be an internal domestic requirement written into the criminal code of both jurisdictions. The Rule would have the force of law, would govern behavior in both jurisdictions, and would be judicially accepted in both jurisdictions. The validity of the Rule, for the purpose of extradition, would be unquestioned. Satisfaction of the dual criminality requirement would permit ex-

²⁰⁰ In the EU, where data protection concerns predominate, reporting of beneficial owner information is lawful where there is a legal obligation. See Council Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 6(1)(c), 2016 O. J. L 119/1 [hereinafter GDPR] ("Processing shall be lawful [if] processing is necessary for compliance with a legal obligation to which the controller is subject").

²⁰¹ 74 Fed. Reg. 57593, 57594 (2009).

²⁰² APUNCAC arts. 19(10–11), 39(1), 40(1).

²⁰³ *Id.* art. 40(7).

²⁰⁴ *Id.* arts. 30, 40 (3, 7).

²⁰⁵ 31 CFR §§ 595.204, 595.701(a)(2).

tradition from one APUNCAC State Party to another. Once extradition had been obtained, prosecution would proceed.

The process would begin when a court in the requesting state issues an arrest warrant for a violation of the Rule. A prosecutor in the requesting state would seek extradition of an accused person to the custody of the requesting state. An accused person may challenge extradition via a habeas petition. However, a habeas review of an extradition certification order in U.S. extradition is “limited to whether: (1) the extradition magistrate had jurisdiction over the individual sought, (2) the treaty was in force and the accused’s alleged offense fell within the treaty’s terms, and (3) there is ‘any competent evidence’ supporting the probable cause determination of the magistrate”.²⁰⁶ Since the extradition magistrate is a magistrate of the requested jurisdiction, rather than a magistrate in the requesting state, there is no test of the jurisdiction of the requesting state except if competent evidence supporting the probable cause determination is lacking.

The bar is not high. “Many modern extradition agreements have not only done away with the requirement for documents to be bound and sealed, but have also dispensed with the requirement to prove a *prima facie* case on the request” (Seddon et al. 2021, p. 569). The European Arrest Warrant, for example, requires “a box to be ticked indicating a Framework List offense is the subject of the request, together with a short description, usually no more than a paragraph, of the conduct alleged against the requested person” (Seddon et al. 2021, p. 569). Other Member States of the Council of Europe likewise do not require evidence of a *prima facie* case in the extradition request (Seddon et al. 2021, p. 569). “All that is required is an affidavit, usually from a state prosecutor, setting out information on which a judge at the extradition hearing can determine whether an extradition offense is [described]” (Seddon et al. 2021, pp. 569–70). “Such affidavits often do no more than recite the conduct imputed to the requested person in the domestic indictment. . . together with the key procedural milestones in the domestic criminal case, the current whereabouts of the person sought, some personal information about them, and details of the relevant local law, charges, [or] indictment” (Seddon et al. 2021, p. 570). Civil law countries, both within and outside the EU, are generally satisfied by “submission of an exposition of the facts”, “without requiring further evidence of the possible involvement or guilt of the requested person” (van der Wilt 2022, p. 31).

A similar criterion is applied in the U.S., a common law jurisdiction. Extradition from the U.S. is not a criminal proceeding (“Orders of extradition are sui generis. They embody no judgment on the guilt or innocence of the accused but serve only to insure [sic] that his culpability will be determined in another and, in this instance, a foreign forum”).²⁰⁷ The magistrate judge’s finding of probable cause is “not a finding of fact ‘in the sense that the court has weighed the evidence and resolved disputed factual issues.’”²⁰⁸ Therefore, the court must uphold the probable cause finding “if there is any competent evidence in the record to support it”.²⁰⁹

Regarding a violation of the APUNCAC Rule, the requesting state would only have to provide competent—i.e., legally admissible—evidence that a front man falsely certified beneficial ownership, or a bank clerk failed to obtain the required beneficial ownership certifications. A text message directing the front man to send or receive funds would be competent evidence that a front man is not the true beneficial owner and a false certification was performed in violation of the Rule. Documentary evidence that a bank clerk failed to obtain the required beneficial owner certifications would be competent evidence supporting a probable cause finding of a violation of the Rule. “[U]nsworn hearsay statements con-

²⁰⁶ Santos v. Thomas, 830 F.3d 987, 1001 (2016) (citing Vo v. Benov, 447 F.3d 1235, 1240 (9th Cir. 2006)); Fernandez v. Phillips, 268 U.S. 311, 312 (1925)); see also United States v. Knotek, 925 F.3d 1118, 1124 (9th Cir. 2019).

²⁰⁷ See Jhirad v. Ferrandina, 536 F.2d 478, 482 (2d Cir. 1976); accord Valencia v. Limbs, 655 F.2d 195, 198 (9th Cir. 1981).

²⁰⁸ Santos, (quoting Quinn v. Robinson, 783 F.2d 776, 791 (9th Cir. 1986)).

²⁰⁹ Id. (quoting Quinn, 783 F.2d, at 791).

tained in properly authenticated documents can constitute competent evidence to support a certificate of extradition".²¹⁰

Extradition does not depend upon an inquiry into the sufficiency of the indictment. In general, it is sufficient if the count in the indictment plainly shows that the defendant is charged with a crime.²¹¹ "Habeas corpus is not the proper procedure to test an alibi or the guilt or innocence of the accused; the sufficiency of the indictment or complaint as a matter of technical pleading is not inquired into on habeas corpus" (Carty 1951, p. 191). In general, comity dictates that requests for extradition are honored unless there is a legitimate reason to deny (Carty 1951, p. 193).

When a state requests another to surrender a fugitive to its jurisdictional control, it asserts jurisdiction over the subject matter of the conduct allegedly performed by the actor (Bassiouni 1974, p. 57). Subject matter jurisdiction may legitimately rest upon application of the effects principle. This representation by the requesting state presupposes that the requesting state is competent to exercise personal jurisdiction over the accused. A request for extradition is an assertion of personal jurisdiction; i.e., an assertion that the requirements for personal jurisdiction would be satisfied upon surrender and transfer of the accused.

A state may punish a defendant for acts committed outside the state if those acts were intended to, and actually did, produce detrimental effects within the state.²¹² "Whenever courts are faced with the problem of acts committed outside [a state's] jurisdiction but having effects within it, the perpetrator is deemed constructively present in the state where the effects of the conduct took place and which requests that actor's delivery" (Bassiouni 1974, p. 14). The U.S. Supreme Court held that "Acts done outside a jurisdiction, but intended to produce and producing detrimental effects within it justified a State in punishing the offender if the State should succeed in getting him within its power".²¹³ The state demanding extradition is justified in asserting personal jurisdiction.

In sum, a nation's extraterritorial prescriptive jurisdiction, i.e., the authority to make its law applicable to persons, conduct, relations, or interests outside its territory, may be justified purely via the effects principle. A law based on the effects principle would provide the basis to arrest an accused person acting outside that territory. Regarding the APUNCAC Rule, it does not matter whether the accused person was acting outside the regulating jurisdiction.²¹⁴ Arrest would be followed by extradition. Extradition is a prerequisite to the establishment of personal jurisdiction (i.e., jurisdictional competence to enforce the law against the accused person). If the requested state agreed, extradition would be obtained, and prosecution would proceed.

The transnational legality of the APUNCAC Beneficial Owner Rule in a transnational case would depend on two elements: (a) applicability of the Rule to the person and situation in question at the time of the act, pursuant to the legal system promulgating the Rule, and (b) acceptability, pursuant to international law, of the application of the Rule in that case (see Gallant 2022, p. 638). This, in turn, would depend on the extent to which extraterritorial application of the Rule is properly founded on the effects principle or the objective territorial principle. If it is properly founded on either principle, then the accused would have a legal duty to obey it (see Gallant 2022, p. 639). The issue is whether extraterritorial application of the Rule to foreign bank clerks and front men would make money laundering substantially less likely in the regulating territory. Disputes about the applicability of the Rule would be adjudicated in courts such as the ECJ. Judicial decisions would set precedents that would shape subsequent decisions. "The International Court of Justice, as well as other international tribunals and municipal courts, . . . rely heavily on judicial precedent" (Janis 2003, p. 83). These courts follow "a doctrine known in France as a *jurisprudence constante*,

²¹⁰ Artukovic v. Rison, 784 F.2d 1354, 1356 (9th Cir. 1986).

²¹¹ Pierce v. Creedy, 210 US 387.

²¹² Strassheim v. Daily, 221 US 280, 285 (1911).

²¹³ *Id.* at 280.

²¹⁴ It does not matter because there is not a conflict of laws. No law prohibits a beneficial owner from certifying beneficial ownership. No law prohibits a bank clerk from submitting a certification required by law.

rendering decisions that are sequentially consistent” (Janis 2003, p. 83). A series of decisions upholding the Rule would affirm the legality of the Rule. If courts uphold the Rule, its international legality would be affirmed and covered individuals would be obliged to observe the Rule or risk the consequences of failure to observe the Rule, including the possibility of arrest, extradition, trial, and imprisonment.

3.30. Extradition, Criminal Prosecution, and Cooperation—Antitrust Model

Cartelists operate across borders to fix prices globally, allocate sales volume among firms globally, and allocate customers globally (Kolasky 2004, pp. 219–20). In these cases, prosecutors must prosecute conduct that occurs outside the regulating territory that has anticompetitive effects within the regulating territory. Antitrust has necessarily served as a testing ground for the application of the effects principle and the practice of asserting extraterritorial jurisdiction over foreign nationals acting outside the regulating territory.

Global application of the effects principle and the practice of asserting extraterritorial jurisdiction and prosecuting foreign nationals is illustrated in antitrust and criminalization of cartel-related offenses, challenging the notion that the effects principle is not globally accepted. “There are more than 130 jurisdictions around the world with a competition law in place” (Burgess 2023, p. 454). Across dozens of jurisdictions, antitrust and cartel-related offenses may be charged as criminal offenses, with criminal penalties. Cartel-related offenses have been criminalized in Australia, Brazil, Canada, Iceland, Indonesia, Israel, Japan, South Korea, Norway, Russia, Thailand, the U.S., Zambia, and a majority of EU member states (Shaffer et al. 2015, p. 312); Mexico, South Korea, and the United Kingdom (Mark 2018, p. 97); Chile, Colombia, and Peru (Gutiérrez 2023, p. 506); Cambodia, Laos, Myanmar, Philippines, and Vietnam (Burgess 2023, p. 470); New Zealand, Saudi Arabia, and South Africa (DLA Piper 2022, p. 8); Malaysia and Taiwan (Jones Day 2012).²¹⁵ Antitrust law offers a strong precedent illustrating the application of criminal penalties to extraterritorial violations of domestic criminal laws.

Country-specific legal and statutory precedents in antitrust clarify the boundaries of international law and practice when prosecutors seek to apply laws based upon the effects principle to foreign nationals acting outside the regulating territory. These precedents suggest that the APUNCAC Rule and its reliance on the effects principle are aligned with international norms and practices. The precedents suggest that the APUNCAC strategy, involving assertions of extraterritorial jurisdiction over bank clerks and front men in offshore havens, is not inconsistent with international law. The precedents suggest that the strategy of applying extraterritorial jurisdiction to pressure recalcitrant offenders into cooperation agreements, where they agree to provide testimony against co-conspirators, is feasible, practical, and sensible.²¹⁶

3.30.1. Acceptance of Effects Principle

Criminalization of cartel offenses has been accompanied by growing acceptance of the effects principle. In cross-border cases, “it has been gradually accepted that a state can apply its competition law to the activities on the basis of the effects within its territory. It is said that ‘virtually all jurisdictions apply some form [of] an effects test’” (Nishioka 2020, p. 591). It is “widely accepted that the application of competition law based on effects in a state’s territory does not contravene public international law” (Nishioka 2020, p. 593). “Such effects prove a genuine link or legitimate interest. A state can consequently apply its competition law as long as any part of the activities occurred in or their effects are felt in its territory” (Nishioka 2020, p. 593). Judicial acceptance of the effects principle is apparent, including jurisdictions outside the U.S. and EU.

²¹⁵ Criminalization may be inferred in countries where penalties include imprisonment.

²¹⁶ If, for example, a bank clerk stated that he was directed by a bank manager ‘not to worry’ about compliance with the APUNCAC Rule, the bank manager would be implicated in a conspiracy to violate the Rule. The criminal penalties attached to violations of the Rule would create strong incentives for bank managers to enforce adherence to the Rule.

Japan

Japan adopted the effects principle to apply Japanese law outside of Japan. “In 2017, the Supreme Court of Japan first decided the international scope of the Japanese Anti-Monopoly Act (JAMA) in cross-border cartel cases and clarified that the JAMA could apply to anti-competitive activities conducted outside of Japan” (Nishioka 2020, p. 590).

The holding shows that, for the application of relevant provisions, it is not required that any of the activities be conducted or implemented in Japan; the JAMA can apply to anti-competitive conduct carried out outside of Japan if the free competition economic order of Japan is disturbed. (Nishioka 2020, p. 598)

In sum, “the Supreme Court has adopted an effects test” (Nishioka 2020, p. 597). “Accordingly, the JAMA will be applied when a cartel causes anti-competitive effects in the Japanese market, even if the action occurs abroad” (Nishioka 2020, p. 605).

Notably, “the JAMA is basically silent on its international or geographical scope. In other words, the JAMA itself does not set any limitation on its scope” (Nishioka 2020, p. 593). “Thus, it is possible to apply the JAMA to cross-border cases as long as such an application is not against public international law” (Nishioka 2020, p. 593). “There seems no doubt that the JAMA may be applied to regulate anticompetitive activity abroad if its effects occur in Japan (Nishioka 2020, p. 595). The JAMA stipulates criminal penalties not to exceed five years imprisonment or a criminal fine not to exceed ¥5 million (Watanabe and Yanagisawa 2019, p. 146).

South Korea

In South Korea, endorsement of the effects principle has been codified in law and court rulings. South Korea amended the Monopoly Regulation and Fair Trade Act (MRFTA) to codify the extraterritorial application of South Korean competition law (Jung 2005, pp. 180, 98). The amendment expressly applies “to acts committed abroad that affect the domestic market”—implying application of the effects principle (Lee et al. 2022, p. 199).²¹⁷ The MRFTA was amended to ensure that it could be used to exercise jurisdiction over such acts—i.e., offenses committed by foreigners in foreign countries having the object or effect of restricting competition within the domestic South Korean market (Jung 2005, pp. 189–90, 98–99). Prior to these amendments, the Seoul High Court affirmed the extraterritorial application of South Korean cartel regulations (Jung 2005, p. 180).

The Court held that when the foreign enterprises entered into an agreement to restrain competition, and the subject of the agreement included the Korean market, regardless of whether the collusive behavior took place inside or outside the territory of Korea, the Court has the jurisdiction to apply Korea’s competition law to the extent that the agreement directly affected the Korean market. The Court appears to have accepted the typical effects doctrine. (Jung 2005, pp. 181–82)

The Court held that extraterritorial application is appropriate because no provision of MRFTA limited “its application to a domestic entity or to acts occurring inside the country” (Jung 2005, pp. 188–89). The Supreme Court of Korea affirmed the application of the effects principle, holding that conduct outside South Korean territory having, or intended to have, significant effect within South Korean territory triggered jurisdiction (Won-cheol 2006, p. 386). In South Korea, participation in cartel activity is punishable by imprisonment not to exceed three years or a criminal fine not to exceed KRW 200 million (Jung 2005, p. 189; Lee et al. 2022, p. 192; Yoon et al. 2016, p. 138). Prosecution has led to imprisonment (Lee et al. 2022, p. 194).

China

In China, the Anti-Monopoly Law of China (AML-China) “is applicable to monopolistic conducts outside the territory of the People’s Republic of China, which serve to eliminate

²¹⁷ MRFTA art. 3.

or restrict competition on the domestic market of China” (Lessambo 2020, p. 155).²¹⁸ “Article 2 of the [AML-China] provides for an extraterritorial doctrine effect” (Lessambo 2020, p. 156). There have been a number of cartel cases where conduct outside of China was found to be in violation of the [AML-China] (Lessambo 2020, pp. 156–65; Liang 2019, p. 60). Bid rigging is a criminal offense punishable by imprisonment of up to three years or a fine (Liang 2019, p. 62). “The longest sentence. . . in a bid-rigging case” was two years and six months (Liang 2019, p. 62).

Vietnam

In Vietnam, “Article 1 of the Competition Law 2018 widens the scope of governance. Accordingly, anticompetitive conduct outside of Vietnam will be caught if such conduct has an actual or potential competition-restraining impact on the domestic market. This is so irrespective of whether the foreign entity has a presence in Vietnam” (Tuan et al. 2019, p. 299). Offenses are criminally prosecutable and may be punished by imprisonment not to exceed five years or a fine not to exceed 3 billion dong (Tuan et al. 2019, p. 301).

Taiwan

In Taiwan, the Fair Trade Law (FTL) “extends to conduct that takes place outside Taiwan if the conduct has an effect on the relevant market in Taiwan” (Ohlson et al. 2013, p. 306). Failure to cease anticompetitive conduct after an initial warning by Taiwan’s Fair Trade Commission (FTC) may be punished by imprisonment not to exceed three years or a fine not to exceed TWD 100 million.

Under Article 35 of the FTL, the FTC may order an enterprise to cease cartel activity, rectify its conduct or take necessary corrective action by a specified deadline. If the enterprise fails to satisfy the order or, after ceasing the cartel activity, commits the same or a similar violation, the criminal sanction for the actor is imprisonment for no more than three years or detention, a fine of not more than NT\$100 million, or both. (Ohlson et al. 2013, p. 307)

Australia

In Australia, the Competition and Consumer Act 2010 (CCA) “prohibits the making of a ‘contract, arrangement or understanding’ containing a cartel provision or the giving effect to a cartel provision contained in a contract, arrangement or understanding” (Clarke 2023, p. 478). “Australian law prohibits [contracts, arrangements, or understandings] which have the purpose, effect or likely effect of substantially lessening competition” (Clarke 2023, p. 481). “Australian competition law applies to conduct that occurs outside Australia. . . if that conduct is carried on by: companies incorporated or carrying on business within Australia” (Oddie and McMahon 2022, p. 7). The law would apply, for example, to an arrangement completed outside Australia, by a company incorporated outside Australia, if the arrangement restricts competition for a product sold by that company within Australia. The arrangement would have the effect of restricting competition within the domestic market. “For individuals, cartel offences are punishable by up to ten years’ imprisonment and/or a fine not exceeding 2000 penalty units (currently AU\$444,000)” (Clarke 2023, p. 495). In June 2022, four individuals involved with money transfer business Vina Money Transfer were the first individuals to be convicted for criminal cartel conduct in Australia, receiving varying terms of imprisonment ranging from nine months to two years and six months” (Oddie and McMahon 2022, p. 9).

Russia

In Russia, domestic anticompetition law captures anticompetitive conduct outside Russia if the conduct has an effect in Russia. “The Competition Law establishes a principle of extraterritoriality. The provisions of this law are applied to agreements reached outside

²¹⁸ Anti-Monopoly Law of China (AML-China), art. 2.

the Russian Federation between Russian and/or foreign entities or organisations, and to their actions, provided that such agreements or actions affect competition in Russia” (Zabrodin and Akimova 2012).²¹⁹ The law would apply, for example, to two foreign entities that completed an agreement outside Russia if the agreement restricted competition within Russia. Offenses may be punished by imprisonment for a term of three to seven years, compulsory labor for a term of three years, or fines of between RUB 300,000 and RUB 500,000 (Zabrodin and Akimova 2012).

Brazil

Brazil applies the effects principle to conduct that produces, or has the potential to produce, the anticompetitive effects listed in Article 36 of the Brazilian Antitrust Act, even if the conduct occurred outside Brazil and the anticompetitive effects were “not achieved”, (de Arruda Sampaio and de Arruda Sampaio 2019, pp. 39–40).

The Brazilian Antitrust Act applies to antitrust violations (even if potential) that occur on Brazilian territory and to those that take place outside Brazilian borders, but may have direct or indirect effects in Brazil. In other words, international cartels that result or may result in direct or indirect effects within Brazilian territory are under CADE’s jurisdiction, even if no illegal conduct is carried out in Brazil.²²⁰ (de Arruda Sampaio and de Arruda Sampaio 2019, p. 40)

In sum, the Act prohibits anticompetitive conduct outside Brazil that has effects within Brazil. Such cartel-related offenses are federal crimes punishable by imprisonment from two to five years, plus a fine (de Arruda Sampaio and de Arruda Sampaio 2019, p. 41).

Argentina

In Argentina, Antitrust Law No. 27.442 (AL) prohibits cartel conduct (Corvalan and Plaza 2022, p. 6). The law applies to extraterritorial conduct if that conduct has a domestic effect within Argentina: “According to Section 4 of the AL, cartels carrying out economic activities abroad are also covered by the prohibition, provided the effects of their conduct produce an effect in the national market” (Corvalan and Plaza 2022, p. 6). Such cartel-related offenses may be punished by imprisonment not to exceed two years or fines (Corvalan and Plaza 2022, p. 8).

Kenya

Kenya applies its own laws, as well as regional common market COMESA laws, to govern extraterritorial conduct that has an effect within Kenya.²²¹ The “COMESA Regulations apply to all economic activities whether conducted by private or public persons within, or having an effect within, the common market” (Kiunuhe and Wagacha 2019, p. 154). The COMESA regulations control extraterritorial conduct outside the COMESA region. “The regime applies to conduct that takes place outside the jurisdiction if it has an effect in the COMESA region” (Kiunuhe and Wagacha 2019, p. 154). In addition, the regime applies to conduct anywhere outside Kenya if the conduct has an effect in Kenya. “The regime applies to conduct that takes place outside the jurisdiction if it has an effect in Kenya” (Kiunuhe and Wagacha 2019, p. 154). Kenya “provides for imprisonment for a term not exceeding five years and a fine not exceeding 10 million Kenya shillings as the criminal penalties for engaging in cartel activity” (Kiunuhe and Wagacha 2019, p. 157).

²¹⁹ Vladislav Zabrodin and Irina Akimova, 2013. Russia. In *Cartel Regulation in 46 Jurisdictions Worldwide 2014*. Edited by A. Neil Campbell. London: Law Business Research, pp. 245–50.

²²⁰ The Administrative Council for Economic Defence (CADE) is the Brazilian antitrust agency responsible for prosecuting and adjudicating cartel cases in the administrative sphere. de Arruda Sampaio and de Arruda Sampaio (2019, p. 39).

²²¹ The Common Market for Eastern and Southern Africa (COMESA) Competition Commission Regulations, the Competition Act 2010, and the East African Community Competition Act 2006 govern economic conduct that has an effect in Kenya. Kiunuhe and Wagacha (2019, p. 152).

Nigeria

In Nigeria, the Federal Competition and Consumer Protection Act (FCCPA) prohibits anticompetitive conduct that affects Nigeria (Balogun et al. 2022, p. 97). “The FCCPA applies to any conduct outside Nigeria by . . . any person in relation to the supply or acquisition of goods or services by that person into or within Nigeria. . . where such conduct has an effect in Nigeria” (Balogun et al. 2022, p. 98). Offenses are punishable by imprisonment not to exceed three years or a fine not exceeding NGN 10 million (Balogun et al. 2022, p. 99).

South Africa

South Africa has been very successful in prosecuting cartel-related offenses. “The South African competition authorities have developed a fairly extensive track record in penalising cartels” (Muzata et al. 2017, p. 13). “South Africa’s aggressive investigation and enforcement against cartel conduct is unparalleled in any of the SACU/SADC countries” (Kaira 2017, p. 79).²²² Cartel behavior is regulated by the South African Competition Act No. 89 of 1998, as amended (Oxenham and Webber 2013, p. 272).

Section 3 of the Competition Act provides that the Competition Act applies to all economic activity within, or having an effect within, South Africa. Thus, cartel conduct occurring outside South Africa (including cartel conduct relating to indirect sales) may be covered by the prohibition where it can be said to have an effect within South Africa. (Oxenham and Webber 2013, p. 273)

Offenses are punishable by imprisonment not to exceed ten years or a fine not to exceed R 500,000.²²³

Summary

In sum, judicial acceptance of the effects principle is apparent, including jurisdictions outside the U.S. and EU. Foreign nationals acting outside Japan, South Korea, China, Vietnam, Taiwan, Australia, Russia, Brazil, Argentina, Kenya, Nigeria, and South Africa are subject to criminal prosecution if their conduct has anticompetitive effects within the domestic markets of Japan, South Korea, China, Vietnam, Taiwan, Australia, Russia, Brazil, Argentina, Kenya, Nigeria, or South Africa. These jurisdictions apply their domestic laws in ways that capture extraterritorial conduct by foreign nationals outside the regulating territory if that conduct has the object or effect of restricting competition within the territory of the regulating state. These precedents suggest that the type of extraterritorial regulation envisioned by the APUNCAC Rule is not incompatible with international law or legal systems in Japan, South Korea, China, Vietnam, Taiwan, Australia, Russia, Brazil, Argentina, Kenya, Nigeria, or South Africa.

3.30.2. Extradition of Foreign Nationals

Prosecution by the U.S. and EU of anticompetitive conduct is especially vigorous. “The United States’ antitrust laws have a broad extraterritorial reach” (Mark 2018, p. 99). The Antitrust Division of U.S. DOJ has been highly successful in extraditing and prosecuting foreign nationals. In 2010, the U.S. successfully obtained extradition of British citizen Ian Norris, the former CEO of Morgan Crucible plc, who exhausted his final appeal in European courts after years of challenging DOJ’s request that he be extradited to stand trial for price-fixing and obstruction of justice in connection with a conspiracy involving carbon products (Shaffer et al. 2015, pp. 335–37). While price-fixing was not, at that time, a crime under UK law, obstruction of justice was a crime, satisfying the dual criminality requirement

²²² The Southern African Customs Union (SACU) comprises five Member States: Botswana, Lesotho, Namibia, South Africa and Swaziland. The Southern African Development Community (SADC) comprises 16 Member States: Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic of Tanzania, Zambia and Zimbabwe.

²²³ Competition Act No. 89 of 1998 (South Africa), as amended, §74(a).

for extradition. Norris's extradition was a milestone in DOJ's efforts to prosecute foreign nationals in criminal antitrust cases.

Extradition Is Not Uncommon

Well over a hundred foreign nationals have been extradited to the U.S. (Reims 2022, p. 8). DOJ's long-arm jurisdiction has reached individuals in France, Germany, Japan, Korea, Sweden, Taiwan, the UK and elsewhere (Ezrahi and Kindl 2011, p. 426). The Antitrust Division has successfully applied the extraterritorial provisions of U.S. antitrust law to threaten overseas executives accused of violating U.S. laws with extradition and has secured the surrender of some thirty or more overseas executives by offering them a deal in the form of a substantially reduced jail term (Joshua et al. 2008, p. 361; Krotoski 2015, p. 2; Mark 2018, p. 100). "Foreign defendants from Canada, France, Germany, Sweden, Switzerland, the Netherlands, Norway, United Kingdom, Korea, and Japan have served or are now serving prison terms in the United States for violating U.S. antitrust laws" (Joshua et al. 2008, p. 361). "Foreign executives are increasingly likely to face antitrust charges in the United States" (Mark 2018, p. 108).

While certain jurisdictions decline to extradite their own nationals, the Department of Justice neutralizes the effectiveness of this practice by placing wanted individuals on INTERPOL's Red Notice list. Persons included on INTERPOL's wanted list can be arrested almost anywhere once they are outside their home territory. When they travel across borders, they risk arrest and extradition to the United States.

In 2013, for example, Romano Piscioti, an Italian national and a former senior executive with Parker ITR, a marine hose manufacturer headquartered in Italy, was arrested by Germany while catching a connecting flight at Frankfurt airport (Thomas and Stefano 2016, p. 1). Piscioti was unaware of having been placed on an INTERPOL Red Notice. "He had been indicted 'under seal' (i.e., filed with a court without becoming a matter of public record) in 2012 for various alleged antitrust violations, and was placed on an INTERPOL Red Notice by the U.S. government" (Thomas and Stefano 2016, p. 1). Germany arrested and extradited Piscioti to the U.S. based on a DOJ charge of participating "in a conspiracy to suppress and eliminate competition by rigging bids, fixing prices and allocating market shares for sales of marine hose sold in the U.S. and elsewhere" (Thomas and Stefano 2016, p. 1). "Piscioti pled guilty to the DOJ's charges, resulting in a two-year period of imprisonment and a \$50,000 criminal fine" (Thomas and Stefano 2016, p. 1).²²⁴

Convictions have been obtained "against executives in Germany, Belgium, the Netherlands, England, France, Switzerland, Italy, Canada, Mexico, Japan, and Korea" (Baker 2001, p. 707). Violations are felonies, and an individual can be subjected to a fine of USD 1,000,000 and (or) 10 years imprisonment.²²⁵ "In 1999 and 2000, individual defendants were sentenced to 12,246 days of incarceration (approximately thirty-four years), including fifteen sentences of twelve months or more" (Baker 2001, p. 707). "In fiscal years 1999 and 2000, six foreign nationals were sentenced to serve time in U.S. prisons for antitrust offenses" (Baker 2001, p. 707). "In 2001, the United States entered a plea agreement in which, for the first time ever, a Japanese executive has agreed to face a possible jail sentence for a violation of U.S. antitrust law" (Baker 2001, p. 707). "DOJ has successfully prosecuted foreign antitrust conspiracies involving the automotive, manufacturing, defense and other industries" "and more than 30 foreign executives were sentenced to prison terms" (Freeman and Hickerson 2023).

DOJ continues to state that it is 'committed to ensuring the culpable foreign nationals, just like U.S. co-conspirators, serve jail sentences in order to resolve their criminal liability.' In FY 2011, foreign executives faced average prison sentences of 10 months for antitrust violations. In FY 2012, DOJ continued to obtain long prison sentences for foreign nationals, including a 24-month sentence

²²⁴ United States v. Piscioti, SD Fla. (April 24, 2014).

²²⁵ 15 USC §§ 1–3 (2022).

for two executives of Japan-based Yazaki Corporation, who voluntarily submitted to U.S. jurisdiction, imposed in connection with their involvement in international conspiracies to fix prices for auto parts sold to automobile manufacturers in the United States. (Warin 2013, p. 6)

Dual Criminality Is Satisfied

While extradition is generally contingent on dual criminality, a growing list of countries have criminalized antitrust and cartel-related offenses, thus satisfying the dual criminality requirement. “At least 36 countries imposed criminal liability for cartel activities, including such major economic powers as Australia, Brazil, Canada, France, Germany, Israel, Japan, Mexico, Russia, South Korea, and the United Kingdom” (Mark 2018, p. 97).

The criminalization of cartel offenses means that extradition will become more commonplace in countries other than the U.S. (Shaffer et al. 2015, p. 335). “Individuals now face potential imprisonment for cartel activity in Australia, Brazil, Canada, Iceland, Indonesia, Israel, Japan, Korea, Norway, Russia, Thailand, and Zambia, in addition to the U.S. and a majority of EU member states” (Shaffer et al. 2015, p. 312). In certain EU Member States, the acting persons are punishable by a criminal fine or imprisonment (Reims 2022, p. 5). In the following EU Member States, participation in hardcore cartels is only subject to criminal punishment in the context of procurement processes:

(1) Austria: imprisonment of up to 3 years, (2) Germany: a criminal fine of up to EUR 10.8 million or imprisonment of up to 5 years, (3) Hungary: imprisonment of up to 5 years, (4) Italy: a criminal fine of up to EUR 1032 or imprisonment of up to 5 years and (5) Poland: imprisonment of up to 3 years.²²⁶ (Reims 2022, p. 5)

In the following EU Member States, participation in hardcore cartels is also criminally punishable outside of procurement activities:

(1) Czech Republic: a criminal fine depending on the damage or imprisonment of up to 8 years, (2) Denmark: an unspecified criminal fine, (3) Estonia: a criminal fine of up to 500 days’ income or imprisonment of up to 3 years, (4) France: a criminal fine of up to EUR 75,000 or imprisonment of up to 4 years, (5) Greece: a criminal fine of up to EUR 1 million or imprisonment of up to 2 years, (6) Ireland: a criminal fine of up to EUR 4 million or imprisonment of up to 10 years, (7) Romania: a criminal fine of up to RON 150,000 or imprisonment of up to 3 years, (8) Slovakia: imprisonment of up to 6 years, (9) Slovenia: a criminal fine of up to 500 days’ income or imprisonment of up to 5 years and (10) Spain: a criminal fine of up to 2 years’ income or imprisonment of up to 3 years.²²⁷ (Reims 2022, p. 5)

“Seven countries other than the United States provide criminal liability to both enterprises and individuals—Austria, Canada, Ireland, Israel, Japan, Korea, and Norway. Three others provide criminal sanctions for individuals but not enterprises—France, Greece, and Switzerland” (Baker 2001, p. 710). The provisions for individual criminal sanctions satisfy the requirements for dual criminality, making foreign nationals eligible for extradition.

Latin America

National competition laws have been adopted in 23 Latin American and Caribbean countries, including Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guyana, Paraguay, Peru, Uruguay, and Venezuela (Gutiérrez 2023, pp. 501–2). “The only sovereign state located in South America that lacks a national competition law is Suriname” (Gutiérrez 2023, p. 502). Legislation was inspired by “the Treaty on the Functioning of the European Union (‘TFEU’), the United States’ Sherman Act, [and] the competition laws of European states

²²⁶ An overview of all states with a cartel criminal offense and brief explanations can be found in Shaffer, Gregory C., Nathaniel H. Nesbitt, and Spencer W. Waller, 2015, “Criminalizing Cartels: A Global Trend?”, in *Comparative Competition Law*, edited by John Duns, Arlen Duke, and Brendan Sweeney, pp. 301–44.

²²⁷ *Id.*

such as Spain” (Gutiérrez 2023, p. 505). All South American countries “explicitly prohibit the categories of conduct that are identified with ‘hard-core cartels’: price fixing, market sharing, limiting or allocating output or suppliers and bid rigging” (Gutiérrez 2023, p. 505). Certain offenses are criminal offenses in Colombia, Brazil, Chile, and Peru (Gutiérrez 2023, p. 506). “Criminal enforcement of cartels in Brazil has been significant in recent years”, with over 300 individuals facing criminal prosecution for antitrust offenses in 2015 alone (Gutiérrez 2023, p. 507). Criminal prosecution has increased, leading to convictions and prison sentences (Gutiérrez 2023, p. 507). Criminalization implies that dual criminality is satisfied, and extradition is a threat to fugitives within the relevant jurisdictions.

Southeast Asia

Competition laws extend to Southeast Asia. “Competition laws and policies now exist in all ten ASEAN member states (‘AMS’), i.e., Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam (Burgess 2023, p. 454). “All ASEAN competition laws include prohibitions against cartels” (Burgess 2023, p. 454). The cross-border nature of cartels and the need to prosecute foreign nationals is explicitly recognized (see Burgess 2023, p. 456). The laws of Brunei, Malaysia, and Singapore explicitly focus on the ‘object or effect’ of alleged conduct (Burgess 2023, p. 463). The laws of Brunei and Singapore focus on conduct that has “the object or effect of preventing, restricting or distorting competition” within state territory (Burgess 2023, p. 463). Cambodian law imposes an object or effects test (Burgess 2023, p. 464). “The AMS laws allow for a mix of civil and criminal sanctions for infringements of the cartel provisions” (Burgess 2023, p. 469). “Criminal sanctions for hard-core cartels are provided for in seven of the ten AMS (Cambodia, Indonesia, Lao PDR, Myanmar, Philippines, Thailand and Vietnam)” (Burgess 2023, p. 470). “Imprisonment is provided for in Cambodia, Indonesia, Myanmar, Philippines, Thailand and Vietnam” (Burgess 2023, p. 470). “Singapore, Malaysia, Indonesia and Vietnam have successfully prosecuted cartels, while others have already commenced investigations”(Burgess 2023, p. 475). Criminalization implies that dual criminality is satisfied, and extradition is a threat to fugitives within the relevant jurisdictions.

3.30.3. Enablement of Cooperation Agreements

The establishment of criminal liability and the threat of criminal prosecution means that cartelists have a strong incentive to pursue cooperation agreements, where cartelists who cooperate and agree to testify against other individuals receive immunity from prosecution (Shaffer et al. 2015, pp. 337–38). Since the first cartelist to cooperate is most likely to receive immunity, cartelists “race to confess” their crimes (Shaffer et al. 2015, pp. 337–38). Cooperating witnesses enable the prosecution of recalcitrant offenders, enabling prosecutors to punish individuals who would otherwise escape justice. The effectiveness of cooperation programs has led 60 jurisdictions worldwide to adopt them, “including Australia, Brazil, Canada, Czech Republic, the EU, France, Germany, Ireland, Japan, South Korea, New Zealand, Sweden, and the UK” (Shaffer et al. 2015, pp. 337–38). This phenomenon has been described as “the single most significant development in cartel enforcement”(Shaffer et al. 2015, pp. 337–38).

Japan

In Japan, “an immunity (i.e., leniency) programme is provided under the Antimonopoly Law”(Watanabe and Yanagisawa 2019, p. 148). The first applicant who files prior to initiation of an investigation may receive “total immunity” from criminal sanctions; subsequent applicants (up to five) may receive a 40 percent deduction depending on their degree of cooperation with JFTC investigators (Watanabe and Yanagisawa 2019, p. 148).²²⁸ “The JFTC determines the rate of reduction taking account of the degree of cooperation by

²²⁸ The Japan Fair Trade Commission (JFTC) is the investigator and prosecutor regarding offenses established by the Antimonopoly Law. Watanabe and Yanagisawa (2019, p. 143).

the applicants” (Watanabe and Yanagisawa 2019, p. 148). “Full cooperation is required for the JFTC to grant the leniency (i.e., all of the relevant information must be disclosed and all of the evidence available to the applicant must be produced for the JFTC)” (Watanabe and Yanagisawa 2019, p. 149).

South Korea

In South Korea, “The first applicant to voluntarily self-report illegal cartel conduct through the KFTC’s leniency and amnesty programmes may be fully exempted from penalty surcharges and criminal prosecution” (Lee et al. 2022, p. 192).²²⁹ “Leniency will be granted to only the first or second applicants to the KFTC” that meet conditions including “the applicant fully cooperates with the KFTC throughout the investigation by stating all facts concerning the cartel and submitting relevant documents” (Lee et al. 2022, p. 196). These provisions encourage insiders who have knowledge of cartel activities to negotiate cooperation agreements with the KFTC.

China

In China, “Article 46 of the [AML-China] provides the legal basis for a leniency regime, which gives SAMR or local PMRD discretion to reduce or waive penalty for. . . participating in a cartel if they voluntarily report the relevant facts and provide material evidence” (Liang 2019, p. 64).²³⁰ “An application for mitigated penalty or exemption from penalty may be filed in accordance with the law” (Liang 2019, p. 65).

The term ‘material evidence’ refers to evidence which may lead to the launch of an investigation by SAMR or local PMRD or makes an essential contribution to the finding of a cartel agreement, including: the identities of undertakings as parties to monopoly agreements; scope of commodities concerned; content and method of conclusion of the monopoly agreement; and actual implementation of the monopoly agreement. (Liang 2019, p. 65)

“SAMR or local PMRD shall decide whether to give a mitigated penalty or exempt the undertaking from penalty by considering the factors including. . . the degree of importance of the evidence provided” (Liang 2019, p. 65). “For the first applicant in a case, the anti-monopoly law enforcement agency may exempt such undertaking from penalty or reduce the fine amount by not less than 80 percent” (Liang 2019, p. 65).

Vietnam

In Vietnam, “the Competition Law 2018 provides for a leniency programme, under which co-conspirators participating in a cartel may turn themselves in and assist with the NCC’s investigation in exchange for either full immunity from, or a reduction of, fines for breach of competition law which the NCC would have otherwise imposed on them” (Tuan et al. 2019, p. 303).²³¹ “Only three whistleblowers are eligible for leniency, with the first entitled to full immunity, while the second and third shall receive a 60 percent and 40 percent fine reduction respectively” (Tuan et al. 2019, p. 303). “To qualify for leniency an applicant must. . . provide all evidence of the infringement which is significantly valuable to dismantle the cartel [and] cooperate fully with the competition authority during the investigation” (Tuan et al. 2019, p. 303). “Emphasis will be placed on the quality of evidence provided. . . Examples of evidence which may prove useful to the investigators include, for instance, a signed agreement or memorandum, an implicating email/instant message exchange between the cartel participants, or a voice recording or minutes of a discussion

²²⁹ The Korea Fair Trade Commission (KFTC) investigates, prosecutes, and adjudicates MRFTA offenses. Yoon et al. (2019, p. 162).

²³⁰ The State Administration for Market Regulation (SAMR) and the market regulatory departments of people’s governments of all provinces, autonomous regions and municipalities directly under the Central Government Provincial Market Regulatory Department (PMRD) investigate cartel matters. Liang (2019, p. 59). Under the AML-China, SAMR renders decisions independently without relying on the court. *Id.*

²³¹ The National Competition Commission (NCC) investigates and adjudicates administrative competition violations.

on competitively sensitive topics (e.g., pricing scheme) between them” (Tuan et al. 2019, p. 303).

Taiwan

In Taiwan, “the Regulations on Immunity and Reduction of Fines in Illegal Cartel Activity Cases” empower the Fair Trade Commission (FTC) “to reduce or entirely waive administrative fines that would otherwise be imposed on enterprises participating in a cartel” (Oxenham and Webber 2013, p. 308). “A leniency or immunity applicant must provide concrete evidence that can assist the FTC in initiating an investigation. . . or establishing that the enterprises involved have participated in a cartel” (Oxenham and Webber 2013, p. 309). Complete immunity may only be granted if an applicant is the first to apply and has met specified conditions (Oxenham and Webber 2013, p. 309). The magnitude of penalty reduction is conditioned on whether an applicant is the first, second, third, or fourth applicant that satisfies specified FTC conditions, including “honest, full and continuous assistance in the investigation from the time the application is filed until the case is concluded” (Oxenham and Webber 2013, p. 309).

Australia

In Australia, “cooperation is a matter to be considered in sentencing and has attracted considerable discounts in criminal cases to date including a 50 per cent discount in the first criminal cartel decision” (Clarke 2023, p. 498). “Civil immunity is available only to the first eligible party to disclose the cartel conduct; other parties may seek to cooperate with the ACCC to achieve a reduction in subsequent penalty” (Clarke 2023, pp. 497–98).²³²

Russia

In Russia, “Relief from criminal liability is possible for each cartel participant, provided [specified] conditions have been fulfilled [including] the cartel participant contributed to solving such a crime” (Zabrodin and Akimova 2012). “Only the entity that was first to fulfil all the conditions set forth in the . . . Administrative Violations Code can be released from liability” (Zabrodin and Akimova 2012).

If for any reason a defendant is unable to satisfy all requirements necessary to be released from criminal liability, it is also possible in theory to conclude a pre-judicial agreement in cooperation with the prosecutor after a criminal case has been initiated. In the event all conditions of the pre-judicial agreement on cooperation, surrender, active contribution to resolving and investigating a crime, exposure of other criminal participants and search for property are fulfilled, and provided there are no aggravating circumstances, the scope of punishment cannot exceed half the maximum term or half the amount of the strictest punishment for a respective cartel crime. (Zabrodin and Akimova 2012) (citations omitted)

Brazil

In Brazil, “a successful leniency application. . . entitles individuals for full immunity against the antitrust criminal prosecution” (de Arruda Sampaio and de Arruda Sampaio 2019, p. 43). To qualify, an applicant must be the first to apply for leniency in relation to the disclosed violation and must fulfill conditions including “full and permanent cooperation with the investigation and respective administrative process, attending any investigation action when requested. . . and the cooperation results in the identification of the other participants involved in the violation; and information and documents that prove the disclosed violation” (de Arruda Sampaio and de Arruda Sampaio 2019, p. 43). “The applicant of a leniency agreement must provide evidence supporting the disclosed violation and shall cooperate fully with the investigation” (de Arruda Sampaio and de Arruda

²³² The Australian Competition and Consumer Commission (ACCC) is the nation’s independent government agency tasked with enforcement of the CCA.

Sampaio 2019, p. 44). “The cooperation will influence the amount of [penalty discount] . . . the more evidence provided, the greater the discount” (de Arruda Sampaio and de Arruda Sampaio 2019, p. 44). Brazil’s prosecuting agency (CADE) has the authority to negotiate and execute a leniency agreement with an applicant (de Arruda Sampaio and de Arruda Sampaio 2019, p. 45).²³³ Over a 12 month period, CADE negotiated 44 leniency agreements and 29 settlement agreements (de Arruda Sampaio and de Arruda Sampaio 2019, p. 46).

Argentina

Argentina has established a leniency program.

[The] programme grants (i) full immunity to the first applicant as long as the applicant provides the authorities with significant evidence, (ii) a reduction of between 20 per cent and 50 per cent of the fine imposed on other applicants, depending on the type of information and evidence provided for the analysis of the case, and (iii) a supplementary benefit, known as leniency plus, consisting of a reduction by one-third of the fine or sanction that would otherwise have been imposed as a result of the petitioner’s participation in the first conduct, if the petitioner reveals a second, different, cartel in the investigation. (Corvalan and Plaza 2022, p. 8)

“To obtain full immunity, the petitioner must comply with” conditions that include full cooperation with Argentina’s National Commission for the Defence of Competition (CNDC), which conducts investigations and applies the Antitrust Law (Corvalan and Plaza 2022, p. 8).

Kenya

In Kenya, “the Leniency Programme Guidelines. . . provide for a leniency programme. . . to parties that report cartel conduct” (Kiunuhe and Wagacha 2019, p. 159). “Parties that report cartel conduct are offered a full or a partial reduction of the administrative financial penalty imposed by the CAK depending on when they report” (Kiunuhe and Wagacha 2019, p. 159).²³⁴ “The importance of being the first applicant for leniency or ‘the first through the door’, is that the applicant is granted 100 percent reduction in the administrative financial penalty, which is also termed ‘immunity’” (Kiunuhe and Wagacha 2019, p. 159). “An applicant for leniency is expected to ensure total cooperation with the CAK throughout the investigation and until a determination by the CAK” (Kiunuhe and Wagacha 2019, p. 160).

Nigeria

In Nigeria, “The FCCPC introduced a leniency programme. . . [that] regulates how persons (natural and juristic) may cooperate and assist the FCCPC in investigations and benefit from reduced penalties, non-prosecution or immunity as the FCCPC may determine” (Corvalan and Plaza 2022, p. 99).²³⁵

South Africa

South Africa’s Corporate Leniency Policy (CLP) is “intended to be a policy designed to encourage disclosure by offering immunity from penalisation for cartel conduct in terms of the Competition Act” (Kaira 2017, p. 80). South Africa’s Competition Commission is entrusted with the responsibility of investigating and prosecuting cartel behavior and is “empowered under the Act to adopt and implement the CLP by granting conditional and total immunity to parties who aid the Commission by providing evidence to enable it to

²³³ The Administrative Council for Economic Defence (CADE) is responsible for prosecuting and adjudicating cartel cases in the administrative sphere. de Arruda Sampaio and de Arruda Sampaio (2019, p. 39).

²³⁴ The Competition Authority of Kenya (CAK) investigates and prosecutes cartel offenses and imposes pecuniary penalties. Kiunuhe and Wagacha (2019, p. 152).

²³⁵ The Federal Competition and Consumer Protection Commission (FCCPC) is Nigeria’s regulatory and enforcement authority regarding all anti-competitive and consumer protection matters. Corvalan and Plaza (2022, p. 97).

tail cartels and stop them” (Mahlangu 2014, p. 20). “As an incentive for co-operation, the Commission grants immunity to a cartel member who is first to approach the Commission and self-confess about its participation in the cartel conduct” (Mahlangu 2014, p. 14). “[I]mmunity involves the Commission granting a promise to an applicant whom it awards immunity that it will not surrender that applicant to adjudication before the Tribunal for its involvement in the prohibited conduct” (Mahlangu 2014, p. 14). In general, immunity is conditional—“the applicant must fully co-operate with the Commission because the Commission may still revoke immunity on the grounds that the applicant no longer conforms to the requirements of the CLP” (Mahlangu 2014, p. 17). These provisions have been highly successful in eliciting cooperation with Commission investigations. “[T]he CLP has been the single most decisive factor in facilitating a successful cartel enforcement regime in South Africa” (Kaira 2017, p. 79). The CLP “has led to the disclosure of many cartels which the Commission would not have discovered due to their nature of secrecy” (Mahlangu 2014, p. 20).

3.30.4. Summary

In sum, there are ample precedents—including precedents in Asia, Latin America, and Africa—establishing the viability, practicality, and effectiveness of fighting international organized financial crime by imposing extraterritorial regulations governing the behavior of foreign nationals in their home jurisdictions, attaching criminal penalties, pursuing extradition, prosecuting foreign individuals for violations of the regulations, and obtaining cooperation agreements with key participants. This approach is not inconsistent with accepted principles of international law. It is extremely effective. As noted by a former deputy assistant attorney general in the Antitrust Division of DOJ:

Our experience in the United States has taught us that criminal sanctions are absolutely essential to effective cartel enforcement. There is no more effective deterrent to cartel behaviour than the knowledge that, if caught, the individuals involved will have to serve jail time. Almost as importantly, there is no other effective way to persuade lower level employees to cooperate in an investigation and to supply evidence that will incriminate their superiors, their employers and their co-conspirators. The ability to offer a participant in a cartel either immunity from prosecution or a reduced sentence in exchange for testimony is the prosecutor’s single strongest weapon in cartel enforcement. Without that weapon, most employees would be unwilling, either for reasons of loyalty or because of fear of retaliation or of being ostracised, to ‘fink’ on their fellow executives and co-conspirators. (Kolasky 2004, p. 211)

The Leniency Program has played a major role in the Antitrust Division’s successful prosecution of criminal cartels. As criminal penalties associated with cartel conduct have increased, companies and individuals have more to lose by not being first in the door. Companies become less willing to risk that their cartel activities will go undiscovered or unreported, and more willing to self-report promptly in the hopes that they get the first mover advantage. (Kolasky 2004, p. 212)

3.31. Extraterritorial Regulation—Examples

The extraterritorial regulation of foreign persons, entities, and activities is not uncommon (Zerk 2010, p. 12). Extraterritorial regulation has been adopted unilaterally by regulating states, especially in the area of financial services (Zerk 2010, p. 63). Significantly, foreign persons and entities with minimal nexus to regulating states are increasingly subjected to prescriptive legal requirements regarding offshore financial transactions that largely occur outside the territory of regulating states. “Violations of prescriptive requirements may be punishable by criminal sanctions” (Zerk 2010, p. 64).

This can be understood most clearly through six examples involving (a) extraterritorial application by the U.S. of U.S. money laundering statutes, (b) extraterritorial application

by the U.S. of the U.S. Foreign Account Tax Compliance Act (FATCA), (c) extraterritorial regulation of financial markets via the European Market Infrastructure Regulation (EMIR), (d) extraterritorial regulation of financial markets via the Markets in Financial Instruments Regulation (MiFIR), (e) extraterritorial regulation of financial markets via the Short Selling Regulation, and (f) extraterritorial regulation of financial markets via the Market Abuse Regulation.

Examples (a) and (b) involve the extraterritorial application of U.S. laws to foreign persons and entities outside the territory of the United States. Examples (c), (d), (e), and (f) involve the application of EU financial market regulations beyond the EU. Hadjiyianni notes that “EU law increasingly has an extraterritorial reach”, involving extraterritorial application of EU regulations abroad, devoid of an EU territorial connection ([Hadjiyianni 2021](#), p. 246). The EU has effectively established itself as a global regulatory power, instigating reforms in countries outside the EU via an assortment of unilateral financial regulations ([Hadjiyianni 2021](#), p. 247). Significantly, the established triggers for the application of EU law—EU-related conduct, nationality, or presence—are being supplemented by effects-based and anti-evasion extraterritorial triggers that cause EU law to apply to conduct that occurs outside the EU ([Emmenegger 2016](#), pp. 648–49; [Scott 2014](#), pp. 1343, 57–59). These examples establish precedents for the APUNCAC Rule’s extraterritorial regulation of financial transactions involving APUNCAC State Party nationals, entities, or funds.

Significantly, all six examples illustrate triggers that capture foreign persons and entities merely because they interact with domestic persons, entities, or funds. This type of trigger is now increasingly used by the EU.

A person may incur obligations under EU law not as a result of their own status but as a result of the status of the person or property with whom or with which they transact. In this situation, the person incurring an obligation under EU [law] will have an indirect connection with the EU as a result of the relationship that they have formed with a person or property that has been deemed to be sufficiently closely connected with the EU. ([Scott 2014](#), p. 1360)

These precedents are apposite to the jurisdiction and application of the APUNCAC Rule, which is triggered by funds (i.e., property) sent, received or handled by a person or entity under the jurisdiction of an APUNCAC State Party.

3.31.1. Title 18 Section 1956

The U.S. money laundering statutes have increasingly been used by the U.S. Department of Justice (DOJ) to prosecute crimes with little nexus to the United States ([Gibson Dunn 2020](#), p. 1). DOJ has relied on a broad interpretation of “financial transactions” that occur “in whole or in part in the United States” to reach, for instance, conduct that occurred entirely outside of the United States and included only a correspondent banking transaction that cleared in the United States ([Gibson Dunn 2020](#), p. 1).²³⁶

Establishing a violation of U.S. Title 18 Section 1956 by a non-U.S. citizen abroad requires (a) engagement in a financial transaction, (b) knowledge that the transaction involved proceeds of “specified unlawful activity”, (c) intent to promote specified unlawful activity or conceal the proceeds of specified unlawful activity, and (d) conduct that occurs in part in the United States ([Gibson Dunn 2020](#), p. 2).

Establishing a violation of the APUNCAC Rule by a non-State Party national regarding actions outside the territory of a State Party would require (a) engagement in a covered financial transaction, (b) failure to submit the required beneficial owner certifications (in the case of a bank clerk), or false certification of beneficial ownership (in the case of a front

²³⁶ United States v. Prevezon Holdings Ltd., 251 F. Supp. 3d 684, 692 (SDNY 2017); Decision & Order Denying Motions to Dismiss at 14, United States v. Boustani, No. 1:18-cr-00681 (EDNY October 3, 2019), ECF No. 231.

man), and (c) evidence that the transaction involved funds originating from, or sent to, or handled by, a person or entity within the jurisdiction of an APUNCAC State Party.²³⁷

The prosecution of a Panamanian bank clerk who processed a USD 3000 wire transfer from a State Party (Kenya, for example) but failed to observe the APUNCAC Rule would involve (a) a covered financial transaction, (b) failure to submit the required beneficial owner certifications, and (c) evidence that the transaction involved funds sent from a person or entity within Kenyan jurisdiction.

This would parallel DOJ prosecutions of individuals who are not U.S. nationals but are engaged in financial transactions outside the U.S., where the financial transaction is processed in whole or in part via a connection to a U.S. person or entity. DOJ policy and U.S. court decisions that a U.S. correspondent banking relationship is sufficient to establish U.S. jurisdiction is no different than the argument that funds with a nexus to an APUNCAC State Party are sufficient to establish APUNCAC State Party jurisdiction. The mere fact that funds are processed for a few milliseconds by a correspondent bank operating within U.S. jurisdiction triggers U.S. jurisdiction over parties who send or receive the funds, even though the parties are not U.S. nationals and their activity, except for the correspondent banking process, takes place entirely outside U.S. territory.²³⁸

3.31.2. FATCA

A second example of extraterritorial financial regulation involves the U.S. Foreign Account Tax Compliance Act (FATCA). In 2010, the U.S. implemented FATCA, and in 2012 strengthened the Act, to compel foreign financial institutions (FFIs) that serve U.S.-based individuals to give the U.S. Internal Revenue Service (IRS) specified client account information linked to those individuals.²³⁹ FFIs may either sign an agreement to submit account information directly to the IRS or sign an agreement where account information is submitted to domestic tax authorities who then make the information available to the IRS upon request. An FFI that refuses to sign an agreement triggers 30 percent withholding of all U.S.-source income paid to the FFI. To implement FATCA, the IRS issued rules requiring all domestic entities that remit such income to withhold 30 percent, pending FFI submission of the required client account information to U.S. authorities. This effectively compels each FFI to comply with FATCA's information collection and submission requirements. The IRS utilizes its control over domestic entities that fall within its jurisdiction to exert control over FFIs that would not ordinarily be subject to IRS jurisdiction.

FATCA ingeniously targets FFIs that previously enabled U.S.-based individuals to hide and evade taxes on U.S.-source income by parking those funds in secret offshore bank accounts. FATCA creates an onerous reporting and paperwork burden on foreign financial institutions that previously aided and abetted tax evasion.

Similarly, the APUNCAC Rule would create a reporting requirement that would apply to financial service personnel who handle covered funds emanating from, or received by, a person or entity within the jurisdiction of an APUNCAC State Party. The Rule would apply to financial service personnel regardless of their territorial location, regardless of their jurisdictional location, and regardless of whether they reside or work within the territory of an APUNCAC State Party. The extraterritorial application of the APUNCAC Rule would be no different than the extraterritorial application of FATCA.

²³⁷ A bank clerk who willfully violated the APUNCAC Rule would necessarily intend to promote a violation of a legal requirement.

²³⁸ *Prevezon*, 251 F. Supp. 3rd, at 693. The sender and recipient of the funds involved in the transactions were foreign parties whose activities were conducted outside U.S. territory and had no connection to the U.S. except that the funds were channeled through correspondent banks located in the United States. *See also* Decision & Order Denying Motions to Dismiss at 14, *United States v. Boustani*. The court held that correspondent banking transactions occurring in the United States are sufficient to satisfy the jurisdictional requirements of 18 USC § 1956(f).

²³⁹ Foreign Account Tax Compliance Act, Pub. L. No. 111-147, 124 Stat. 71, 97-117 (2010) (codified at 26 USC §§ 1471-1474, § 6038D (2016)).

3.31.3. EMIR

U.S. and EU regulations regarding trading in financial derivatives have considerable extraterritorial effects in other parts of the world. Even if parties have little or no connection to the U.S. or the EU, a transaction may be subject to U.S. or EU regulations if a transaction is deemed to have a significant effect on the U.S. or the EU (Chen 2017, pp. 334–35). For example, transactions in East or Southeast Asia, involving East or Southeast Asian parties, may be subject to U.S. or EU regulations (Chen 2017, pp. 337–39). The extraterritorial effects of U.S. and/or EU regulations can hardly be avoided.

The European Market Infrastructure Regulation (EMIR) is an example of a financial regulation that exerts extraterritorial control over certain transactions involving non-EU parties.²⁴⁰ The impetus for EMIR was the 2008 financial crisis (Coffee 2014, p. 1263). AIG was unable to meet margin calls related to trading in OTC derivatives, threatening global financial contagion and collapse (Coffee 2014, p. 1262). In recognition of the interconnected nature of derivatives trading, the EU implemented EMIR.

EMIR regulates any EU investment or insurance entity that serves as a counterparty and counterparties to those entities.²⁴¹ Each counterparty must report details of each derivative contract to a central authority.²⁴² Central counterparties are subject to “frequent and independent audits”.²⁴³ Records must be made available upon request to a central authority.²⁴⁴ On a daily basis, counterparties must “mark-to-market” the value of outstanding contracts, must have risk-management procedures, and must maintain appropriate levels of capital.²⁴⁵

Significantly, EMIR also regulates trades between non-EU entities that have a “direct, substantial and foreseeable effect” within the EU or where it is necessary to guard against evasion of EMIR.²⁴⁶ This extraterritorial provision aligns with the logic of the APUNCAC Rule: extraterritorial regulation is necessary to fight money laundering, which has a direct, substantial and foreseeable effect on crime affecting APUNCAC States Parties, and the concern that it is necessary to guard against evasion of the international anti-money laundering regime. The extraterritorial application of EMIR and the APUNCAC Rule are justified on the basis that extraterritorial behavior has significant domestic effects and the view that extraterritorial control is needed to guard against regulatory evasion.

Significantly, EMIR captures non-EU parties and entities merely because they interact with EU persons or entities.

A clearing obligation will attach to third country entities when they enter into a relevant contract with an EU (financial) counterparty. Here, the third country counterparty is viewed as enjoying an indirect connection with the EU, by virtue of its decision to enter into a transaction with a counterparty that is authorized or established within the EU. This indirect connection is treated as sufficient to justify the imposition of obligations under EU law. (Scott 2014, p. 1360)

“[T]he mere fact of entering into a transaction with an EU-connected person is sufficient to spark the application of EU law” (Scott 2014, p. 1361).

EMIR authorizes the Member States of the European Union to prescribe penalties for noncompliance and “take all measures necessary to ensure that [EMIR rules] are implemented”.²⁴⁷ This implies that any entity that serves as a counterparty but fails to observe the EMIR regulation could be prosecuted by an EU Member State. Presumably, EU Member States would only prosecute offenders whose actions affect, or potentially affect, the EU

²⁴⁰ Council Regulation 648/2012 (European Market Infrastructure Regulation), 2012 O. J. L 201/1 [hereinafter EMIR].

²⁴¹ *Id.* arts. 2(1), 2(8).

²⁴² *Id.* art. 9(1).

²⁴³ *Id.* art. 26(8).

²⁴⁴ *Id.* art. 29(3).

²⁴⁵ *Id.* arts. 11(2), 11(3), 11(4).

²⁴⁶ *Id.* art. 4(1)(a)(v).

²⁴⁷ *Id.* art. 12(1).

community. However, EMIR authorizes any EU Member State to prosecute any person or entity deemed to be in violation of EMIR, regardless of territorial location, where it is necessary to guard against evasion of EMIR. Presumably, EU Member States would utilize “all measures necessary”, including extradition of recalcitrant individuals operating outside EU territorial jurisdiction.²⁴⁸

The rationale for extraterritorial regulation is that financial markets are inextricably intertwined. As demonstrated by the 2008 financial crisis, a failure of regulation in any single jurisdiction can affect the economic well-being of citizens outside that jurisdiction. The need to establish regulations that control extraterritorial behavior is clear.

Similarly, the APUNCAC Rule seeks to regulate behavior that occurs outside the territory of a State Party. The rationale is the same. The existing failure to adequately regulate the behavior of financial service personnel and front men in offshore locations is a primary reason that money laundering persists, the crimes enabled by money laundering persist, and rampant crime involving transnational criminal organizations persists.

3.31.4. MiFIR

The Markets in Financial Instruments Regulation (MiFIR) is another example of a financial regulation that exerts extraterritorial control over certain transactions involving non-EU parties.²⁴⁹ In addition to EU counterparties, MiFIR imposes obligations on non-EU counterparties “provided that the contract has a direct, substantial and foreseeable effect within the Union or where such obligation is necessary or appropriate to prevent the evasion of any provision of this Regulation”.²⁵⁰ The rationale is the same rationale for EMIR and the APUNCAC Rule: there is a need to regulate extraterritorial conduct by parties outside the territory of EU Member States (or, in the case of APUNCAC, outside the territory of APUNCAC States Parties) that has a direct, substantial, and foreseeable domestic effect or where such conduct facilitates evasion of existing laws.

3.31.5. Regulation 236/2012

The Short Selling Regulation is an example of a financial regulation that exerts extraterritorial control over certain transactions involving non-EU parties based on a connection with EU-related property.²⁵¹ This regulation imposes notification and disclosure requirements on entities that hold net short positions in shares and imposes restrictions on uncovered short sales in relation to shares admitted to trading on a trading venue in the EU, even where the shares in question are traded outside an EU venue.²⁵² This regulation illustrates a jurisdictional trigger based on EU-related property, rather than an EU-related person. “It does not matter who is trading in the shares in question or where the transaction takes place” (Scott 2014, p. 1362). “It is the connection that is forged between the shares and the EU—at the point when the shares are admitted to trading on an EU trading venue—that triggers the application of EU law” (Scott 2014, p. 1362).

Reliance on the property principle as a jurisdictional trigger occurs when the EU exercises jurisdiction over transactions on the basis that the property involved in those transactions has a close and specified link with the EU. Where the EU relies on the property principle, the identity of the parties engaging in a transaction is not jurisdictionally salient and nor is the location in which the transaction takes place. . . [T]he property that forms the basis for the exercise of jurisdiction by the EU [may take] the form of financial instruments including, for example, sovereign debt or shares. (Scott 2014, p. 1361)

²⁴⁸ *Id.* art. 12(1).

²⁴⁹ Council Regulation 600/2014 (Markets in Financial Instruments Regulation), 2014 O. J. L 173/84 [hereinafter MiFIR].

²⁵⁰ *Id.* art. 28(2).

²⁵¹ Council Regulation 236/2012 (Short Selling Regulation), 2012 O. J. L 86/1.

²⁵² *Id.* arts. 5, 6, 12.

Regulation 236/2012 is apposite to the APUNCAC Rule. The jurisdictional trigger is covered property rather than the presence of a covered party. In both cases, the involvement of regulated property triggers jurisdiction and application of the relevant rule.

3.31.6. Regulation 596/2014

The Market Abuse Regulation is another example of a financial regulation that exerts extraterritorial control over certain transactions involving non-EU parties based on a connection with EU-related property.²⁵³

This measure prohibits insider trading and market manipulation, and imposes additional obligations on a range of actors including issuers of financial instruments, market operators and persons who professionally arrange transactions in financial instruments. The Regulation applies to financial instruments that are admitted to trading on a regulated market in at least one Member State, or for which a request for admission has been made, as well as financial instruments that are traded on a multilateral trading facility or an organized trading facility in at least one EU Member State.²⁵⁴ It also extends to financial instruments whose price or value depends on or has an effect on the price or value of a financial instrument traded on an EU market.²⁵⁵ Significantly, from a territorial point of view, this Regulation applies to all of these EU-connected instruments (property), even when they are being traded outside an EU trading venue, including in relation to transactions that take place abroad.²⁵⁶ (Scott 2014, p. 1362)

Regulation 596/2014 is apposite to the APUNCAC Rule. The jurisdictional trigger is covered property rather than the presence of a covered party. In both cases, the involvement of regulated property triggers jurisdiction and application of the relevant rule.

3.31.7. Summary of Extraterritorial Regulations

The six examples presented above illustrate the extraterritorial application of domestic laws related to financial transactions. Four of the six examples involve the global application of EU law by EU member states, including civil law jurisdictions. Global application necessarily implies application across civil as well as common law jurisdictions and jurisdictions that mix principles of Islamic, civil, and common law.

These extraterritorial financial regulations seek to control extraterritorial conduct that has foreseeable adverse domestic effects. These regulations capture foreign persons and entities merely because they interact with domestic persons, entities, or funds. Increasingly, domestic laws contain triggers that serve to extend the global reach of those laws to govern conduct that takes place entirely abroad by persons and entities with little or no connection with the jurisdictions promulgating those laws. The rationale is the need to control the behavior, conduct, and actions of individuals and entities that would otherwise be unregulated and would have direct, substantial, and foreseeable adverse domestic effects or where regulation is necessary or appropriate to prevent the evasion of laws designed to protect domestic jurisdictions.

Significantly, Regulation 236/2012 and Regulation 596/2014 establish precedents where the jurisdictional trigger is covered property rather than the presence of a covered party. In both cases, the involvement of regulated property triggers jurisdiction and application of the relevant rule. The parallel with the proposed APUNCAC Rule is clear. The APUNCAC Rule would be triggered and would be applied whenever funds are sent from, or received by, a person or entity within the jurisdiction of an APUNCAC State Party.

The adoption of the APUNCAC Rule would be no different than the adoption of the U.S. Sherman Act, the U.S. money laundering statutes, or any other law or regulation that

²⁵³ Council Regulation 596/2014 (Market Abuse Regulation), 2014 O.J. L 173/1.

²⁵⁴ *Id.* art. 2(1)(a–c).

²⁵⁵ *Id.* art. 2(1)(d).

²⁵⁶ *Id.* art. 2(1)(c).

involves an assertion of extraterritorial control. Those laws are domestic laws that enable the prosecution of non-citizens of regulating states who violate those laws anywhere in the world.

In sum, there are now ample precedents for extraterritorial regulations, such as the APUNCAC Rule, that are intended to prevent harm. Whether the Rule would be enforceable would ultimately depend on court rulings, but the multitude of regulatory precedents suggest that the Rule would indeed be judicially accepted. The fact that six extraterritorial financial regulations have been implemented into law challenges the notion that they are not properly founded on accepted principles of international law. Whether the basis is the objective territorial or the effects principle is immaterial. All six regulations seek to prevent transboundary harm as well as the materialization of harm. The international acceptance of these regulations suggests that there is no conflict with international law or lack of acceptance of this type of extraterritorial financial regulation.

3.32. International Agreements to Exchange Beneficial Ownership Information

International agreements and regulations to collect, report, and exchange beneficial ownership information are common, indicating broad international recognition that this type of agreement and regulation is necessary and desirable. These agreements and regulations include: (a) IOSCO MOU, (b) EOIR/AEOI exchange of information, (c) CARE, (d) 6AMLD, (e) Regulation 2015/847, and (f) TFR.

3.32.1. IOSCO MMoU

In May 2002, the International Organization of Securities Commissions (IOSCO) implemented the Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU).²⁵⁷ Of 159 eligible national regulatory authorities, 129 are MMoU signatories, indicating global endorsement across 129 national regulatory authorities (IOSCO 2023).²⁵⁸ The MMoU obliges the signatory authorities to cooperate regarding the exchange of information required to investigate possible violations of the securities-related laws and regulations of MMoU signatory states. These laws regulate practices including “misrepresentation of material information and other fraudulent or manipulative practices”.²⁵⁹

The purpose is to enforce and secure compliance with the respective laws and regulations of MMoU signatory states.²⁶⁰ The MMoU overrides any domestic secrecy or blocking laws or regulations that would otherwise prevent the collection and transmission of specified information to an MMoU requesting authority.²⁶¹ The signatories agree to “provide each other with the fullest assistance permissible to secure compliance with the respective Laws and Regulations” of the signatory states.²⁶² This assistance includes, without limitation, “obtaining information and documents regarding the matters set forth in the request for assistance”, including “records that identify: the beneficial owner and controller, and for each transaction, the account holder”, plus “information identifying persons who beneficially own or control non-natural Persons organized in the jurisdiction” of the requested state.²⁶³ Significantly, “assistance will not be denied based on the fact that the type of conduct under investigation would not be a violation of the Laws and Regulations of the Requested Authority”.²⁶⁴

²⁵⁷ Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information, *opened for signature* May, 2002 (revised May 2012) [hereinafter MMoU].

²⁵⁸ A notable signatory is France’s *Autorité des marchés financiers* (AMF), indicating broad international acceptance even in jurisdictions with strong blocking statutes.

²⁵⁹ MMoU at 2.

²⁶⁰ *Id.* at 3.

²⁶¹ *Id.* at 3.

²⁶² *Id.* at 4.

²⁶³ *Id.* at 4.

²⁶⁴ *Id.* at 5.

The MMoU establishes a precedent apposite to the APUNCAC Rule. The MMoU is an international agreement to exchange transaction-level information, including the names of specified account holders and beneficial owners, for the purpose of enforcing and securing compliance with domestic securities-related laws and regulations. These laws and regulations prohibit misrepresentation of material information and other fraudulent or manipulative practices. The MMoU overrides domestic secrecy or blocking regulations that would otherwise prevent the collection and transmission of this information to a requesting authority. Exchange of information cannot be denied based upon a dual criminality requirement.²⁶⁵

Similarly, APUNCAC is a model international agreement that would, via the APUNCAC Rule, oblige entities in requested states to collect and transmit transaction-level information regarding beneficial ownership, for the purpose of enforcing and securing compliance with requesting state laws and regulations prohibiting misrepresentation of beneficial ownership and manipulation of the financial system to launder illicit funds. A difference is that the APUNCAC Rule would involve extraterritorial regulation. However, there is ample precedent for this type of unilateral extraterritorial regulation (see Section 3.31, above). Broad international endorsement of the MMoU indicates international agreement that this type of regulation, seeking to enforce compliance with laws prohibiting misrepresentation of beneficial ownership and manipulation of the financial system to launder illicit funds, is necessary and desirable.

International consensus regarding the need for this type of regulation is articulated in Article 7 of UNTOC:

Each State Party: (a) Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions. . . in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions.²⁶⁶

The nearly universal adoption of UNTOC indicates international consensus regarding the need to ensure the proper identification of accurate beneficial owner information. Adoption of the APUNCAC Rule would serve to implement the Article 7 mandate, ensure proper identification of beneficial owners, and close gaps in the international anti-money laundering regime that permit funds to be transmitted in ways that obscure beneficial ownership.

3.32.2. EOIR/AEOI

The Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) involves 165 member states that have committed to two standards. The standards commit members to Exchange of Information on Request (EOIR) and annual Automatic Exchange of Financial Account Information (AEOI) between national tax authorities.²⁶⁷

EOIR requires entities and financial institutions within each member state to collect and, upon demand, report individual beneficial ownership, accounting, and banking information that is to be internationally exchanged upon member state request (OECD 2016, pp. 21–24; 2021, pp. 22, 28). “The standard requires that jurisdictions exchange information with all relevant partners” (OECD 2016, fn 32). The EOIR standard states that “jurisdictions should not decline a request on the basis of its secrecy provisions” (OECD 2016, p. 22; 2021, p. 28). The requested information is to be provided “regardless of the existence of a domestic tax interest or the application of a dual criminality standard” (OECD 2016, pp. 16, 24).

AEOI requires entities and financial institutions within each member state to collect and report information regarding “controlling persons”, i.e., beneficial owners, and their account and bank information; this information is automatically exchanged with tax au-

²⁶⁵ *Id.* at 5.

²⁶⁶ UNTOC art. 7(1)(a).

²⁶⁷ In total, 165 jurisdictions have committed to EOIR; 121 jurisdictions have committed to AEOI.

thorities where the controlling person/beneficial owner is tax resident (OECD 2018, p. 29; 2021, p. 19; Owens and McDonell 2018, p. 30).²⁶⁸ Detailed guidance defines “beneficial ownership” with regard to an array of entities and situations (OECD 2021). The Common Reporting Standard (CRS) governs AEOI information exchanges and imposes financial institution due diligence and reporting obligations regarding customer accounts (Owens and McDonell 2018, p. 30).

All Global Forum members have agreed to be assessed via peer review for their implementation of the EOIR standard (OECD 2016, p. 27). Peer reviews were conducted of all member jurisdictions to assess adherence to the EOIR standard (OECD n.d.b). Upon completion of the review process, each jurisdiction received an overall rating of compliance (OECD n.d.b). Failure to address deficiencies will affect future ratings. The ratings have a reputational impact (OECD n.d.a). Development banks may make investments conditional on ratings and reviews, and the G20 and the EU may use results when establishing their policies (OECD n.d.a).

The commitment of 165 Global Forum members to EOIR/AEOI establishes a precedent apposite to the APUNCAC Rule. Member states have agreed to collect and exchange individual beneficial ownership, accounting, and banking information for the purpose of enforcing and securing compliance with requesting state tax laws and regulations. EOIR/AEOI overrides domestic secrecy laws that would otherwise prevent the collection and submission of this information to a requesting authority.

Similarly, APUNCAC involves a model international agreement that would, via the APUNCAC Rule, oblige entities in requested states to collect and report information regarding beneficial ownership for the purpose of enforcing and securing compliance with requesting state laws and regulations.

The broad agreement of 165 nations to collection, reporting, and international exchange of beneficial ownership information signifies broad agreement that this type of regulation is necessary and desirable to combat evasion of requesting state laws and regulations. EOIR/AEOI focuses on compliance with tax laws and regulations, whereas the APUNCAC Rule is motivated by a concern regarding money laundering. However, the focus of EOIR/AEOI on the collection, reporting, and international exchange of beneficial ownership information parallels the APUNCAC Rule’s focus on the collection and international reporting of beneficial ownership information. Broad international endorsement of EOIR/AEOI indicates international agreement that this type of regulation, requiring collection, reporting, and international exchange of beneficial ownership information, is necessary and desirable to combat evasion of requesting state laws and regulations.

Jurisdictions that have implemented AEOI include Albania, Antigua and Barbuda, Aruba, Azerbaijan, The Bahamas, Barbados, Bermuda, British Virgin Islands, Bulgaria, Cayman Islands, China, Colombia, Costa Rica, Cyprus, Dominica, Ecuador, Estonia, France, Germany, Grenada, Guernsey, Hong Kong, Ireland, Isle of Man, Italy, Jamaica, Jersey, Kazakhstan, Kenya, Kuwait, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau, Maldives, Malta, Mexico, Monaco, Nigeria, Oman, Pakistan, Panama, Peru, Qatar, Romania, Russia, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Saudi Arabia, Seychelles, Sint Maarten, Slovak Republic, Slovenia, Spain, Switzerland, Trinidad and Tobago, Turks and Caicos Islands, United Arab Emirates, and United Kingdom (OECD 2023, p. 1). The list includes most of the high-risk money laundering jurisdictions of concern. The significance is that these jurisdictions have already agreed to implement—and are already implementing—regulations that require collection, reporting, and international exchange of beneficial ownership information. This signifies broad international agreement among key jurisdictions that this type of regulation is necessary and desirable to combat the evasion of requesting state laws and regulations.

²⁶⁸ The term “controlling person” has the same meaning as “beneficial owner” under the FATF Recommendations. Therefore, financial institutions are required to identify the controlling persons/beneficial owners of the account holder in accordance with the FATF Recommendations.

3.32.3. CARF

In August 2022, OECD coordinated with G20 countries to promulgate changes in rules and regulations via the Crypto-Asset Reporting Framework (CARF) that require participating jurisdictions to collect, report, and automatically exchange information regarding the identities of individual beneficial owners and their crypto-asset transactions (OECD 2022). The annual, standardized, international exchange of information with taxpayer jurisdictions-of-residence is intended to protect the international financial system from financial crime, including tax crime, and combat evasion of domestic tax laws and regulations.

Subparagraph D(10) defines “controlling person” to correspond with the term “beneficial owner” as described in Recommendation 10 and the Interpretative Note on Recommendation 10 of the FATF Recommendations (as adopted in February 2012) (OECD 2022, pp. 20, 55). The term is to be interpreted in a manner consistent with the FATF Recommendations (OECD 2022, p. 55). CARF requires participating jurisdictions to collect and report the identities of controlling persons involved in crypto–fiat currency transactions, crypto–crypto transactions, and crypto–retail payment transactions (OECD 2022, p. 15). The Common Reporting Standard (CRS) that governs AEOI information exchanges was revised to cover crypto assets and ensure that information required by CARF will be reported and exchanged with the relevant jurisdictions where controlling persons are resident (OECD 2022, pp. 63, 72, 73, 77, 87–90).

The significance is that—with minor exceptions—all entities within Global Forum jurisdictions are now required, via EOIR/AEOI, to collect and report beneficial ownership information for an array of financial transactions, including certain retail payment transactions, that will be internationally exchanged with relevant tax jurisdictions. The broad agreement of 165 nations to collect, report, and exchange beneficial ownership information for this array of financial transactions signifies broad agreement that this type of regulation is necessary and desirable to combat evasion of domestic laws and regulations. The agreement of 165 nations regarding the necessity and desirability of collecting and automatically exchanging detailed beneficial owner information sets a clear precedent for the type of automatic collection and international reporting of beneficial owner information envisioned by the APUNCAC Rule.

3.32.4. 6AMLD

In December 2022, the European Commission and Council of the European Union agreed upon the 6th Anti-Money Laundering Directive (6AMLD). 6AMLD revises the existing AML regulatory regime (5AMLD). 6AMLD will require credit and financial institutions, with the exception of crypto-asset service providers, to identify the beneficial owner when funds are transacted with a minimum value of EUR 1000, report any discrepancies vis-à-vis information found in central registers, and “refrain from carrying out a transaction” whenever they are “unable to comply” with the requirement.²⁶⁹ Beneficial owner identification would be verified via collection of an identity document such as a passport, or via “the use of electronic identification” that meets “substantial” or “high” levels of assurance.²⁷⁰

The significance of the proposed regulation is that it signals a consensus among EU member states that it is necessary, desirable, and appropriate to impose an international beneficial owner reporting requirement on transactions beyond a threshold amount and to require that a transaction be rejected if beneficial owner information cannot be obtained. This establishes a precedent for the APUNCAC Beneficial Owner Rule, which would impose an international beneficial owner reporting requirement on transactions beyond a threshold amount and require that a transaction be rejected if beneficial owner information cannot be obtained.

²⁶⁹ Commission Proposal for a Council Regulation on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, arts. 15(2), 16(1)(b), 16a(1), 17(1), 2021/0239 (COD) [hereinafter 6AMLD].

²⁷⁰ *Id.* art. 18(4).

3.32.5. Regulation 2015/847

Council Regulation 2015/847 requires payment service providers to reject a transfer of funds unless the transfer is accompanied by verified information regarding the beneficial sender.²⁷¹ The Regulation applies to transfers of funds in any currency that are sent or received by a payment service provider established in the EU.²⁷² The Regulation does not apply to transfers of funds carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, where that card, instrument or device is used exclusively to pay for goods or services; and the number of that card, instrument or device accompanies all transfers flowing from the transaction.²⁷³ However, the Regulation applies when a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, is used in order to effect a person-to-person transfer of funds.²⁷⁴ An EU Member State may decide not to apply the Regulation to transfers of funds where the payment service provider is able to trace back, by means of a unique transaction identifier, the transfer of funds from the payor to the payee, and the amount of the transfer does not exceed EUR 1000.²⁷⁵ This exempts certain low-value transfers of funds used for the purchase of goods or services.²⁷⁶ In sum, the Regulation applies to certain transfers of funds that exceed the transaction threshold and are used for the purchase of goods or services, as well as other specified transfers of funds.

Regulation 2015/847 parallels the APUNCAC Beneficial Owner Rule, which would require payment service providers to reject a transfer of funds unless the transfer is accompanied by verified information regarding the beneficial sender. Regulation 2015/847 signals a consensus among EU member states that it is necessary, desirable, and appropriate to impose a regulation that causes payment service providers to reject a transfer of funds unless the transfer is accompanied by identification of the beneficial owner and submission of beneficial owner information.

3.32.6. TFR

In June 2022, the European Parliament, the Commission, and the Council agreed upon the Transfer of Funds Regulation (TFR).²⁷⁷ TFR will require payment service providers, including crypto-asset service providers (CASPs), to reject a transfer of funds unless the transfer is accompanied by verified information regarding the beneficial sender.²⁷⁸ TFR parallels the APUNCAC Beneficial Owner Rule, which would require payment service providers to reject a transfer of funds unless the transfer is accompanied by verified information regarding the beneficial sender. TFR signals a consensus among EU member states that it is necessary, desirable, and appropriate to impose a regulation that would cause payment service providers to reject a transfer of funds unless the transfer is accompanied by identification of the beneficial owner and submission of beneficial owner information.

3.33. Implications

Section 3.31 describes domestic financial regulations with triggers that extend the global reach of those regulations to govern conduct that takes place entirely abroad by persons and entities with little or no connection with the jurisdictions promulgating those

²⁷¹ Council Regulation 2015/847 on Information Accompanying Transfers of Funds and Repealing Regulation 1781/2006, arts. 4(4), 4(5), 4(6), 2015 O.J. L 141/1.

²⁷² *Id.* art. 2(1).

²⁷³ *Id.* art. 2(3).

²⁷⁴ *Id.* art. 2(3).

²⁷⁵ *Id.* art. 2(5).

²⁷⁶ *Id.* at 3.

²⁷⁷ Commission Proposal for a Council Regulation on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast), 2021/0241 (COD) [hereinafter TFR].

²⁷⁸ *Id.* arts. 4(4), 4(5), 4(6). Regarding the identity of the payer, art. 4(5a) cites 6AMLD art. 16, which requires obliged entities to “identify the beneficial owner”, and art. 18(3), which requires obliged entities to establish the identity of the beneficiary at the time of payout.

regulations. Sections 3.32.1 and 3.32.2 describe international agreements to collect, report, and exchange beneficial ownership information for the purpose of enforcing and securing compliance with domestic laws and regulations. Section 3.32.3 describes an international agreement to collect and automatically report beneficial ownership information for an array of financial transactions, including certain retail payment transactions, that will be internationally exchanged with relevant tax jurisdictions. Sections 3.32.4–3.32.6 describe international agreements to impose regulations that would cause financial institutions and payment service providers to reject transactions if beneficial owner information cannot be obtained.

These precedents indicate international agreement that extraterritorial financial regulation for the purpose of enforcing and securing compliance with domestic laws and regulations is necessary, appropriate, and desirable. The precedents indicate agreement that collection, reporting, and international exchange of beneficial ownership information is necessary, appropriate, and desirable. The precedents indicate agreement that collection and international reporting should extend to an array of financial transactions, including certain retail payment transactions, and financial institutions and payment service providers should reject transactions if beneficial owner information cannot be obtained.

In sum, these precedents signify increasing international agreement that the type of financial regulation represented by the APUNCAC Rule is necessary, appropriate, and desirable to enforce and secure compliance with domestic laws and regulations. The precedents indicate a collective judgment that benefits outweigh costs, protection of the financial system outweighs concerns regarding transaction friction, and existing digital technology is adequate to implement the regulatory requirements.

The U.S. and the EU member states are leaders in establishing and promoting this type of financial regulation. Significantly, the establishment of this type of regulation influences the adoption of similar regulations across the globe. “The Brussels Effect refers to the EU’s unilateral power to regulate global markets. Without the need to use international institutions or seek other nation’s cooperation, the EU has the ability to promulgate regulations that shape the global business environment” (Bradford 2020, p. xiv). The size and attractiveness of the EU market, in combination with a desire to streamline internal operations, causes multinational corporations to respond to EU regulations by aligning their global conduct to EU rules (Bradford 2020, p. 2). After multinational corporations have aligned their conduct to conform to EU rules, they have an incentive to lobby for EU-style regulations in their home jurisdictions (Bradford 2020, p. 2). This ensures that they are not at a disadvantage when competing domestically against companies that do not compete directly in the EU market and, therefore, have no incentive to conform their conduct to costly EU regulations (Bradford 2020, p. 2). Thus, market forces compel multinational firms to lobby for domestic regulations that align with EU regulations, resulting in the de facto adoption of EU regulations across the globe (Bradford 2020, p. 2).

The significance of the precedents described in Section 3.32 is two-fold. Not only is there international consensus across major nations regarding the need to establish regulations regarding the collection and international reporting of beneficial ownership information, suggesting strong international support for the type of regulation represented by the APUNCAC Rule, but the establishment of the APUNCAC Rule by the U.S. and EU member states may be expected to cause the de facto adoption of the APUNCAC Rule across the globe via the Brussels Effect.

3.34. Benefits vs. Costs

Would the benefits of the APUNCAC Rule exceed costs? The imminent implementation of 6AMLD, which will require credit and financial institutions, with the exception of crypto-asset service providers, to identify the beneficial owner when funds are transacted with a minimum value of EUR 1000, report any discrepancies vis-à-vis information found in central registers, and reject a transfer of funds whenever they are “unable to comply”

with the requirement, indicates consensus among EU member states that benefits would exceed costs regarding implementation of the 6AMLD beneficial owner reporting rule.

Implementation of Council Regulation 2015/847, requiring payment service providers to reject a transfer of funds unless the transfer is accompanied by verified information regarding the beneficial sender, indicates consensus among EU member states that benefits exceed costs regarding implementation of the Regulation 2015/847 beneficial owner reporting rule.

The June 2022 agreement among the European Parliament, the Commission, and the Council regarding the Transfer of Funds Regulation (TFR), which requires payment service providers, including crypto-asset service providers (CASPs), to reject a transfer of funds unless the transfer is accompanied by verified information regarding the beneficial sender, indicates consensus among EU member states that benefits would exceed costs regarding implementation of the TFR beneficial owner reporting rule.

OECD and G20 agreement to promulgate changes in rules and regulations via the Crypto-Asset Reporting Framework (CARF) that require participating jurisdictions to collect, report, and automatically exchange information regarding the identities of individual beneficial owners and their crypto-asset transactions indicates consensus among OECD and G20 nations that benefits would exceed costs regarding implementation of the CARF beneficial owner reporting rule.

The global endorsement across 129 national regulatory authorities of the IOSCO MMoU, which obliges the signatory authorities to cooperate regarding the exchange of records regarding beneficial ownership, indicates consensus across 129 national regulatory authorities that benefits exceed costs regarding implementation of the MMoU beneficial owner reporting rule.

The global endorsement by 165 member states of the Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) regarding EOIR/AEOI, which obliges member states to collect, report, and automatically exchange beneficial owner information with tax authorities where the beneficial owner is tax resident, indicates consensus among 165 member states that benefits exceed costs regarding implementation of the EOIR/AEOI beneficial owner reporting rules.

There is consensus among EU member states, OECD member states, G20 countries, 129 national regulatory authorities, and 165 member states of the Global Forum that benefits exceed costs regarding international implementation of beneficial owner reporting rules that are strikingly similar to the proposed APUNCAC Beneficial Owner Rule.

The rationale for the establishment of international beneficial owner reporting rules is stated in the preamble of Regulation 2015/847:

Flows of illicit money through transfers of funds can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorist financing and organised crime remain significant problems which should be addressed at Union level. The soundness, integrity and stability of the system of transfers of funds and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds or to transfer funds for criminal activities or terrorist purposes.²⁷⁹

[T]he Union should ensure that the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by FATF on 16 February 2012 (the ‘revised FATF Recommendations’)... are implemented uniformly throughout the Union... Uncoordinated action by Member States acting alone in the field of cross-border transfers of funds could have a significant

²⁷⁹ Reg. 2015/847 at 1.

impact on the smooth functioning of payment systems at Union level and could therefore damage the internal market in the field of financial services.²⁸⁰

The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, detection and investigation of money laundering and terrorist financing.²⁸¹

While the precise benefits and costs of these rules are not easily quantified, it is clear from the overwhelming adoption of these rules that there is an international consensus that benefits exceed costs. There is a consensus that transnational organized crime typically involves money laundering, money laundering is facilitated when beneficial ownership is obscured, and beneficial owner reporting rules promote transparency and, therefore, promote efforts to fight organized crime. Ultimately, a cost–benefit analysis must weigh the expected value of reductions in human trafficking, sex trafficking, drug trafficking and all other violent and nonviolent crimes facilitated by money laundering, against the administrative, operational, and transaction friction costs of beneficial owner reporting rules. If the expected value of benefits exceeds the expected costs, society benefits when the rules are implemented. The overwhelming international adoption of beneficial owner reporting rules implies a collective judgment that benefits exceed costs.

3.35. *Complicated Ownership Structures*

Ownership structures may be complicated, complicating determinations about the beneficial owners covered by the Rule. For example, preferred shareholders may be enfranchised if their dividend payments are delayed but may otherwise be excluded from voting. The inclusion of preferred shareholders in an evaluation of beneficial ownership might reduce the controlling share of any single shareholder below the 25 percent threshold for the determination of beneficial ownership. This type of issue would be best addressed by rule of FINCEN.

Regardless, the focus of the Rule on transactions simplifies the analysis. If less than five individuals have ultimate control over a given financial transaction, those individuals may be presumed, for the purpose of applying the Rule, to meet the definition of beneficial ownership. Personnel who implement a transaction under the direction of another person are not true beneficial owners and would not be eligible to certify beneficial ownership.

3.36. *Database Security*

Unlike proposals for publicly accessible beneficial owner registries, the APUNCAC Rule beneficial owner information would be transmitted to and stored in a secure, restricted access database operated by a global version of the Financial Crimes Enforcement Network (FINCEN).²⁸² Access would be restricted to authorized personnel under tightly controlled conditions. Authorized personnel would be vetted. Access would be compartmentalized, tracked, and subject to random audits, with penalties for unauthorized use.

Access would be restricted to avoid compromising ongoing criminal investigations, to ensure the privacy of innocent parties and to protect against malicious activity, including industrial espionage. While journalists have demanded publicly accessible registries, premature publication can tip off suspects and compromise investigations. Public access could also facilitate targeting of wealthy individuals and compromise costly investments in sensitive technologies such as extreme ultraviolet lithography.²⁸³

²⁸⁰ *Id.* at 1–2.

²⁸¹ *Id.* at 2.

²⁸² APUNCAC art. 19(2).

²⁸³ For example, a competitor might utilize publicly available registry information to compile a list of ASML suppliers. From this list, a competitor might deduce a list of proprietary industrial ingredients and processes used by ASML in its lithography process, enabling the competitor to replicate the ASML process.

3.37. Political Concerns

If necessary, each State Party could be permitted to name (for example) a maximum of two other States Parties whose investigators would be excluded when conducting sensitive FINCEN database queries related to nationals of that State Party (Yeh 2020c, p. 461). For example, if State Party A does not trust investigators from State Party B, State Party A could exclude investigators from State Party B from conducting sensitive FINCEN inquiries into the activities of nationals of State Party A. The FINCEN database controls could then be set to exclude access by excluded investigators and permit access by the trusted set of investigators when conducting investigations related to nationals of State Party A. Any State Party wishing to pursue an investigation related to nationals of State Party A would be required to rely on the approved set of investigators to conduct FINCEN database inquiries involving nationals of State Party A. Approved investigators would be obligated by APUNCAC to provide mutual assistance in conducting FINCEN database inquiries upon request. This system would permit sensitive FINCEN database inquiries while assuaging concerns about industrial espionage.

3.38. Intercepted Communications

Text messages may be obtained by prosecutors from seized electronic devices. In general, law enforcement authorities may obtain a court order permitting them to seize electronic devices, unlock them, and access text messages.²⁸⁴ In some cases, the devices are in use and not locked when they are seized. In other cases, law enforcement personnel may induce suspects to unlock their devices in exchange for leniency or may utilize a device designed to unlock their phones (Franceschi-Bicchierai 2022). In practice, it is not uncommon for law enforcement personnel to unlock devices to access their contents (Casey 2002; Fukami et al. 2021).²⁸⁵

Accused individuals who reside in a non-cooperating jurisdiction could not evade prosecution if they travel beyond that jurisdiction and are arrested and extradited. Any personal devices in their possession would be seized and transferred to the control of the prosecuting authority.

Communications may also be intercepted via court-authorized electronic intercepts or surveillance. Both civil, as well as common law jurisdictions permit court-authorized electronic intercepts and the installation of surveillance cameras and microphones. In France, for example, a public prosecutor may request a telephone intercept for up to one month or installation of surveillance cameras and microphones in a suspect's home (Hodgson 2012, p. 131). An analysis of legal frameworks in 24 nations found that court-authorized intercepts were permitted in cases of serious crime (SS8 Networks n.d.).²⁸⁶

²⁸⁴ The U.S. Supreme Court has ruled that authorities must obtain, via a court order, a search warrant to access cell phone data and text messages. A court will not issue a search warrant in the absence of probable cause that a crime was committed. A court can issue a remote access search warrant if the location of the device or data is in an unknown location and its location has been concealed via technological means. In situations in which a device is known to be located extraterritorially, the territorial limits on the U.S. warrant authority continue to apply, and U.S. courts lack the authority to issue a warrant to search. Rather, law enforcement is, as a general matter, told to instead employ the mutual legal assistance process and seek the assistance of the government where the data or device is located, irrespective of the foreign government's willingness to cooperate. In the absence of foreign government permission, a search cannot be performed on a device that is known to be outside U.S. territory.

²⁸⁵ While front men and money mules may be supplied with burner phones to foil authorities, this tactic would fail to protect the users if they are in possession of the phones when arrested. In addition, 160 jurisdictions now require mandatory SIM card registration, i.e., users must supply their real names and personal details to activate phone service. While front men and money mules may be instructed to use coded language to foil authorities, this tactic would not protect users if they choose to cooperate with authorities to match specific coded instructions to specific actions, i.e., sending funds in response to the coded instructions.

²⁸⁶ Jurisdictions included Australia, Austria, Argentina, Belgium, Brazil, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Republic of Korea, Netherlands, New Zealand, Norway, Philippines, Poland, Romania, South Africa, Sweden, United Kingdom, and the United States.

In addition, 68 nations are parties to the Convention on Cybercrime ([Council of Europe 2023](#)).²⁸⁷ Article 21, regarding the interception of electronic content, states that each State Party shall empower its competent authorities to intercept real-time communications.²⁸⁸

Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: (a) collect or record through the application of technical means on the territory of that Party. . . content data, in real-time, of specified communications in its territory transmitted by means of a computer system.²⁸⁹

A smartphone is defined as “a device that combines a cell phone with a handheld computer” ([Dictionary.com 2023](#)). This implies that Article 21 applies to smartphones. States Parties have agreed that real-time interception of communications via smartphones and computers, including audio and text messages, is permissible.

Article 9 of the second protocol to the Convention provides for the expedited disclosure, from one State Party to another State Party, of stored computer data, without a request for mutual legal assistance.²⁹⁰ Article 14 of the second protocol specifies that Parties bound by existing international agreements regarding the protection of personal data shall remain bound by those agreements.²⁹¹ Parties may mutually determine the conditions under which data transfer would occur.²⁹² Otherwise, each Party shall consider that the processing of personal data “meets the requirements of its personal data protection legal framework for international transfers of personal data, and no further authorisation for transfer shall be required under that legal framework”.²⁹³

In principle, this implies that a State Party could obtain a court order, then utilize the Convention and the second protocol to the Convention as the legal basis to request copies of intercepted electronic communications, thereby obtaining evidence of instructions directing a front man to send or receive funds in violation of the APUNCAC Rule. The Convention facilitates and promotes the collection and sharing of the type of evidence needed to prosecute financial service personnel and front men who enable money laundering in offshore jurisdictions. It would only be necessary to ensnare a few cooperating witnesses. A prosecutor could then use the leverage to flip additional witnesses.

While criminals may utilize special darknet software designed to preserve user anonymity, this did not prevent authorities from arresting Ross William Ulbricht, who created and operated the Silk Road darknet website ([FBI n.d.](#)). He is now serving a life sentence.

There are many ways that authorities identify and prosecute darknet criminals ([Cox 2016](#)). Ironically, the use of sophisticated—supposedly impregnable—encrypted phones costing USD 1500 apiece led to thousands of arrests when Europol investigators cracked their networks, seized billions of text messages, and began reading the messages in real time, as they were transmitted ([Caesar 2023](#)). “It has never before been possible to see so vividly how many thousands of criminals talk to one another when they think nobody is listening” ([Caesar 2023](#)). Never had police learned so much in such a short period

²⁸⁷ Convention on Cybercrime, *opened for signature* 23 November 2001 ETS 185 (entered into force 1 July 2004). States Parties include Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Greece, Hungary, Iceland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Moldova, Monaco, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Romania, San Marino, Senegal, Serbia, Slovakia, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Tonga, Turkey, Ukraine, United Kingdom, and the United States.

²⁸⁸ *Id.* art. 21.

²⁸⁹ *Id.* art. 21.

²⁹⁰ Second Protocol to the Convention on Cybercrime, *opened for signature* 12 May 2022, art. 9, ETS 224.

²⁹¹ *Id.* art. 14(1)(b).

²⁹² *Id.* art. 14(1)(c).

²⁹³ *Id.* art. 14(1)(d).

of time. They obtained details about “important figures in organized crime who had been ‘completely unknown’ to them and who must have felt ‘untouchable’” (Caesar 2023). “Suddenly, it was as if somebody had switched on thousands of klieg lights, and ‘we could not only take a picture but a movie’” (Caesar 2023). The effect was described as “like an atomic bomb” (Caesar 2023). “The opening of the Sky application was the most powerful weapon in the history of our fight against organized criminal groups” (Caesar 2023).

Similarly, the UK’s National Crime Agency (NCA) infiltrated the encrypted EncroChat instant messaging communication platform, arrested 746 individuals, seized GBP 54 million in illicit cash, and dismantled entire organized crime groups (NCA 2020). NCA Director of Investigations Nikki Holland stated: “The infiltration of this command-and-control communication platform for the UK’s criminal marketplace is like having an inside person in every top organised crime group in the country” (NCA 2020).

The FBI distributed encrypted Google Pixel phones to criminal groups that included a backdoor, permitting law enforcement to see every text, photo, and video and hear every call that users made without their knowledge (Davis 2021). The FBI ultimately decrypted and read more than 27 million messages on over 12,000 devices, resulting in over 800 arrests, thousands of seizures in over 16 countries, and disruption of Albanian organized crime, the Italian mafia, outlaw biker gangs, drug syndicates, and arms smugglers. In sum, the use of encrypted communication devices served to mislead darknet criminals into thinking that authorities were unable to intercept their communications.

4. Discussion

Six case analyses examined the hypothetical application of the APUNCAC Beneficial Owner Rule to examples that illustrate the range and complexity of money laundering: Danske Bank Estonia, the Vancouver Model, Liberty Reserve, the *hawala* system, online gaming, and Lightning (Yeh 2020c). The cases described six strategies used by criminals to introduce illicit funds into the financial system. Any strategy to control money laundering must control all paths. APUNCAC would implement a strategy designed to control all paths. The strategy relies upon the APUNCAC Beneficial Owner reporting requirement.

The APUNCAC Beneficial Owner Rule requires the true beneficial owner controlling the funds involved in a transaction to certify that he or she is, in fact, the true beneficial owner. When funds are paid, deposited, transferred, or exchanged, the beneficial owner must either be present and must certify beneficial ownership in person, or must be contacted and must certify, under penalty of perjury, that he or she is the true beneficial owner, or must have authorized automatic certification of beneficial ownership of all funds sent from, or received by, his financial accounts. If the funds are paid from one person to another, the receiving person must also certify that he is the true beneficial owner controlling the funds that are received.

Figure 12 diagrams the APUNCAC scheme. The APUNCAC reporting requirement inserts the certification requirement into each covered transaction at the point of the transaction. No covered transaction would be consummated unless the true beneficial owners of the transaction funds are identified and recorded in the FINCEN database,²⁹⁴ or front men choose to pose as true beneficial owners, flout the law, and risk the consequences of flouting the law. Many individuals who are currently willing to participate in money laundering schemes only because the risks are minimal would, upon adoption of APUNCAC, have to assess whether it is worth the risk of falsifying information and being arrested and imprisoned for repeated violations of APUNCAC.

²⁹⁴ The FINCEN database is the database established by APUNCAC for the purpose of collecting and centralizing beneficial ownership information and making the information accessible to financial crime investigators. FINCEN is the Financial Crime Enforcement Network established by APUNCAC and modeled on the US Treasury Department’s FinCEN financial intelligence unit. FINCEN is intended to be an international version of FinCEN.

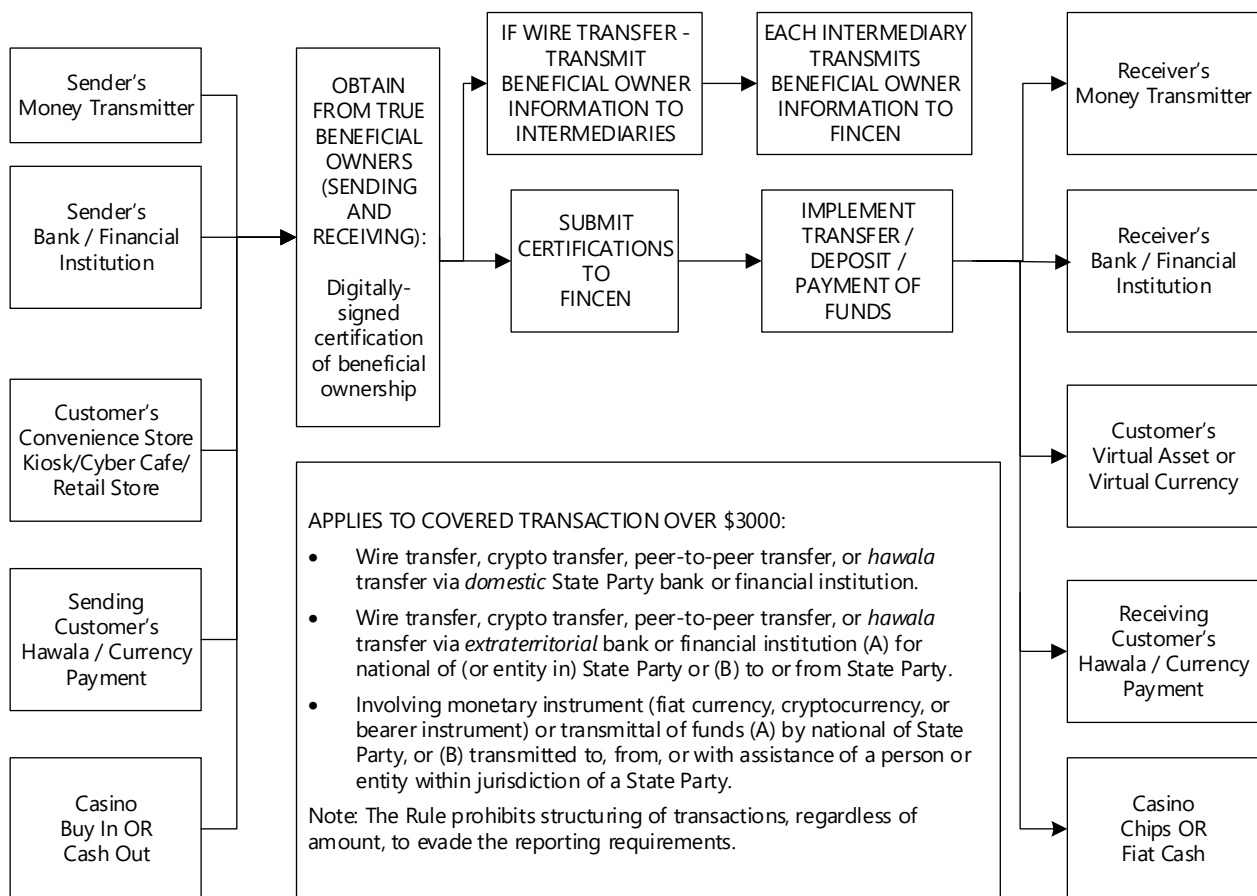


Figure 12. APUNCAC Beneficial Owner Rule.

The rationale for the APUNCAC reporting requirement is that effective investigation and prosecution of corruption and money laundering depends on the capacity of prosecutors to obtain the cooperation of front men, money transmitters, financial institution personnel, and retail clerks who would otherwise aid, abet and facilitate money laundering by processing covered transactions without identifying the true beneficial owner.

The APUNCAC Rule creates a risk of punishment for any front man who participates in a scheme to hide the true beneficial owner when funds are paid, deposited, exchanged, or transmitted internationally. The APUNCAC Rule creates a risk of punishment for any person who assists with a covered financial transaction but fails to obtain and submit the required beneficial owner certifications to FINCEN. This risk of punishment is a necessary element of any effective strategy to control corruption and money laundering. A failure to institute this risk of punishment ensures that prosecutors have little leverage to obtain the cooperation of front men, money transmitters, financial institution personnel, and retail clerks who either actively or passively aid, abet, and facilitate money laundering.

No other anticorruption strategy incorporates the APUNCAC reporting strategy. No other anticorruption strategy criminalizes failure to obtain and submit beneficial owner information, for the array of transactions covered by APUNCAC, to a centralized, online database that is readily searchable by financial crime investigators. The creation of this type of database would expose the identity of criminals seeking to hide illicit gains through complicated transactions involving opaque offshore entities and bank secrecy havens. This type of exposure is necessary to end corruption and impunity. It can only be implemented through changes in laws that create a real risk of arrest and extradition whenever a guilty party travels to a State Party jurisdiction or a jurisdiction that maintains an extradition agreement with a State Party.

In contrast, the existing regulatory regime fails to implement anything like the APUNCAC Rule. In the United States, depository financial institutions are required to verify customer identity when a customer opens a bank account, but the customer is not required to provide a certification, under penalty of perjury, regarding the identity of the actual beneficial owner of the account—the customer is only required to sign a statement that the information that is provided is complete and correct “to the best of” the customer’s knowledge.²⁹⁵ This loophole permits criminals to hide their identities by employing other individuals to open and operate bank accounts that are, in fact, controlled by the criminals. A bank customer who opens an account at the direction of a criminal might choose to assert that he or she (i.e., the customer) was unaware that the account was controlled by another person (i.e., the criminal). The existing regulatory regime does not discourage or prevent this type of deception. The existing system depends on an assertion by the bank customer about the identity of the beneficial owner that may or may not be true.

The APUNCAC Rule closes this loophole. By requiring certification from the actual beneficial owner, instead of a dubious statement from the bank customer, a front man who poses as the beneficial owner is forced to digitally sign a certification of beneficial ownership, under penalty of perjury, that is demonstrably false. It would no longer be possible for criminals to employ individuals to open bank accounts, give false information regarding the beneficial ownership of those accounts and—when questioned—assert that this information was true “to the best of” their knowledge.

The APUNCAC Beneficial Owner Rule cannot be easily foiled by criminals. Criminals who acquire illicit funds use computers and phones to communicate instructions to their front men to open bank accounts and send and receive funds. Prosecutors may seize these devices, unlock them, and gain access to text and email messages that provide independent evidence that the front men listed as beneficial owners are not, in fact, true beneficial owners, because the messages reveal who is controlling the funds. The messages invariably instruct the front men to open bank accounts and send and receive funds. However, a true beneficial owner is the person who gives instructions, not the person who accepts instructions. A front man who accepts instructions cannot be the true beneficial owner who controls the movement of the funds in question. It would be difficult for a front man to maintain the fiction that he is the true beneficial owner. If a front man poses as the beneficial owner, but prosecutors obtain instructions revealing the fakery, prosecutors will have the leverage needed to elicit a cooperation agreement.

Once prosecutors have the evidence needed to prosecute front men, they gain the capacity to pressure front men into cooperation agreements where they reveal the names of the individuals who directed them. Those individuals, implicated in a criminal scheme to hide the identity of the beneficial owner, would presumably cooperate with the prosecutor to avoid imprisonment. The prosecutor would pressure everyone in the chain of individuals to cooperate until the identity of the criminal controlling a transaction is revealed.

Violation of any aspect of the Rule would risk arrest, extradition, debarment, fines, and imprisonment. If front men value their freedom, they will presumably choose to cooperate with prosecutors and reveal details about the individuals who instructed them to serve as front men. Once these individuals are implicated, prosecutors would pressure them into cooperation agreements. Prosecutors would use the information to implicate each person involved in the scheme, pressure them into cooperation agreements, and use the information to prosecute the criminals controlling the scheme.

This strategy is not currently available to prosecutors because existing laws are not designed to ensnare collusive front men via false certifications of beneficial ownership. Consequently, prosecutors do not have the leverage needed to elicit cooperation agreements. In the absence of these cooperation agreements, it is extremely difficult to penetrate

²⁹⁵ 31 CFR § 1010.230 (2017). FinCEN considered and rejected a suggestion that certification be made under penalty of perjury. 81 Fed. Reg. 29398, 29405–6 (2016).

the secrecy that hides the money trail, unravel the fakery, and prosecute the criminals orchestrating the criminal activity.

The APUNCAC Beneficial Owner Rule is a rule that requires submission of information regarding specific transactions, rather than information about the beneficial owners of corporate bank accounts. The APUNCAC Rule lays tripwires that cannot be avoided when criminals seek to use the international financial system to transmit illicit funds offshore. The tripwires take advantage of the fact that criminals must transmit instructions to their agents and front men. The tripwires ensure that agents and front men commit prosecutable offenses if they collude to hide the identity of a criminal who is the ultimate beneficial owner when illicit funds are transmitted.

In contrast, existing laws fail to focus on specific transactions. The focus is, instead, on individuals who open bank accounts. However, criminals can easily avoid any type of account, in any jurisdiction, that might pose difficulties. Criminals will simply choose another type of account in another jurisdiction that has weak beneficial owner identification requirements.

The APUNCAC Beneficial Owner Rule causes that strategy to fail because criminals must necessarily use the international financial system to transmit illicit funds offshore. The APUNCAC Rule lays tripwires that cannot be avoided when funds are transmitted offshore. The tripwires extend beyond the shores of an APUNCAC State Party to the territory of recalcitrant jurisdictions that refuse to join APUNCAC. Conceptually, the tripwires “travel” with the State Party funds wherever they are transmitted.

The direct effects of this type of extraterritorial regulation may be multiplied by indirect effects. The legal risks of noncompliance, plus the operational challenge of separating State Party funds for special treatment, may generate pressure on non-party States to conform domestic regulatory regimes to align with the APUNCAC Rule. Domestic entities may find that it is easier to conform domestic regulations with the APUNCAC Rule so that all transactions are treated in accordance with the Rule, rather than separating transactions into covered and not-covered transactions and treating them accordingly (see [Hadjiyianni 2021](#), p. 253).²⁹⁶ The “Brussels Effect” would have the desired consequence of expanding the APUNCAC Rule across transactions and across borders.

The great benefit of the APUNCAC Beneficial Owner Rule is that it cannot be avoided by any of the usual tactics. Criminals cannot hide behind agents and front men who operate offshore, beyond the reach of domestic authorities. Criminals cannot avoid the APUNCAC tripwires by moving their operations to a jurisdiction that is not a party to APUNCAC. The reason is that criminals generate their illicit funds locally and then seek to transmit them using the international financial system to safe havens. Signature, ratification, and implementation of the APUNCAC Rule is available to any jurisdiction that desires to regain control over funds that are currently being spirited offshore, beyond the reach of domestic authorities, to secrecy havens. A local jurisdiction need only adopt the APUNCAC Rule and pass the necessary conforming legislation. No local jurisdiction needs the cooperation of recalcitrant offshore jurisdictions such as BVI, the Caymans, or Panama.

The implication is that the APUNCAC Beneficial Owner Rule would be a much more effective legal requirement than the existing legal regime for collecting beneficial owner information. The APUNCAC Rule promises to fight money laundering, corruption, and all crimes that utilize money laundering and corruption, and to do so in a way that promises to be vastly more effective than the existing legal regime.

Under APUNCAC, a front man must certify a statement that is demonstrably false, thereby risking debarment, fines, and imprisonment. This risk is not present in the existing regulatory system. The creation of this risk is a necessary step in controlling money laundering and the crimes associated with money laundering. Prosecutors who are unable

²⁹⁶ Hadjiyianni notes that “Non-divisibility of standards favours standardisation over customisation. Bradford usefully uses the example of catering to dinner guests’ dietary requirements. Accommodating the most limiting requirement for all guests is much easier than tailoring each guest’s meal to their own distinct preferences” (p. 253).

to threaten front men have little leverage to obtain their cooperation. In the absence of their cooperation, the identities of the criminals that control illicit funds will remain elusive, the capacity of prosecutors to obtain indictments will remain weak, and criminals will continue to engage in acts of violence, corruption, terrorism, and impunity, facilitated by unimpeded money laundering.

The APUNCAC Beneficial Owner Rule would ensure that prosecutors have the information needed to prosecute financial crime. Efficient prosecution of financial crime would enable prosecution of organized crime and discourage the various types of crime that involve financial crime and organized crime: human trafficking, sex trafficking, drug trafficking, slave labor, child labor, environmental crimes, etc.

The potential social benefits would be enormous. Realization of these benefits depends on recognition of the need for the APUNCAC Beneficial Owner Rule, the availability of solutions to the issues raised by the Rule, and the will to implement the Rule.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The author wishes to thank Clark Abrams, Daniel Gutierrez, Louis de Koker, Athena Kam, Eliseo Martinez, Oonagh McDonald, Kenneth Murray, Stephen Stirling, and Vivian Yuan for helpful comments.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

5AML	5th Anti-Money Laundering Directive (EU)
6AML	6th Anti-Money Laundering Directive (EU)
ACCC	Australian Competition and Consumer Commission
ACH	Automated Clearing House
AEOI	Automatic Exchange of Financial Account Information
AI	Artificial Intelligence
AL	Antitrust Law No. 27.442 (Argentina)
AML	Anti-Money Laundering
AML-China	Anti-Monopoly Law of China
AMS	ASEAN Member States
APUNCAC	Anticorruption Protocol to the United Nations Convention against Corruption
ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
AU	African Union
AWT	Arrest Warrant Treaty
BO	Beneficial Owner
BVI	British Virgin Islands
CADE	Administrative Council for Economic Defense (Brazil)
CAK	Competition Authority of Kenya
CARF	Crypto-Asset Reporting Framework (EU)
CARICOM	Caribbean Community
CASP	Crypto-Asset Service Provider
CCA	Competition and Consumer Act 2010 (Australia)
CEO	Chief Executive Officer
CIDR	Central Identification Data Repository (India)
CLP	Corporate Leniency Policy (South Africa)
CNDC	National Commission for the Defence of Competition (Argentina)
COMESA	Common Market for Eastern and Southern Africa
CRPC	<i>Comparution sur Reconnaissance Préalable de Culpabilité</i> (France)
CrPC	Code of Criminal Procedure (Pakistan)
CRS	Common Reporting Standard
CVC	Convertible Virtual Currency

DNI	National Identity Document (Argentina)
DOJ	U.S. Department of Justice (U.S.)
ECJ	European Court of Justice
ECOSOC	United Nations Economic and Social Council
e-KTP	(electronic) <i>Kartu Tanda Penduduk</i> (Indonesian Residential Identity Card)
EMIR	European Market Infrastructure Regulation
EOIR	Exchange of Information on Request
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
FATCA	Foreign Account Tax Compliance Act (U.S.)
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation (U.S.)
FCCPA	Federal Competition and Consumer Protection Act (Nigeria)
FCCPC	Federal Competition and Consumer Protection Commission (Nigeria)
FFI	Foreign Financial Institution
FINCEN	Financial Crimes Enforcement Network (proposed)
FinCEN	Financial Crimes Enforcement Network (U.S.)
FSB	Federal Security Service (Russian Federation)
FTC	Fair Trade Commission (Taiwan)
FTL	Fair Trade Law (Taiwan)
G20	Group of 20 (19 nations + European Union)
Gavi	(formerly) the Global Alliance for Vaccines and Immunization
GDPR	General Data Protection Regulation (EU)
ICAO	International Civil Aviation Organization
ICIJ	International Consortium of Investigative Journalists
ICN	<i>Identificação Civil Nacional</i> (Brazilian National Identification System)
ICT	Information and Communications Technology
IDC-ID	Interoperable Digital Credential for Legal Identity (Africa)
INTERPOL	International Criminal Police Organization
IOSCO	International Organization of Securities Commissions
IRS	Internal Revenue Service (U.S.)
ITU	International Telecommunication Union
IVTS	Informal Value Transfer Systems
JAMA	Japanese Anti-Monopoly Act
JFTC	Japan Fair Trade Commission
KFTC	Korea Fair Trade Commission
KYC	Know Your Customer
LTDC	Legal Tender Digital Currency
MiFIR	Markets in Financial Instruments Regulation
MLAT	Mutual Legal Assistance Treaty
MMoU	Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (IOSCO)
MNO	Mobile Network Operator
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOSIP	Modular Open Source Identity Platform
MRFTA	Monopoly Regulation and Fair Trade Act (South Korea)
MSB	Money Services Business
NCA	National Crime Agency (UK)
NCB	National Central Bureau
NCC	National Competition Commission (Vietnam)
OCG	Organized Crime Group
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control (U.S.)
OICT	United Nations Office of Information Communications Technology
PCIJ	Permanent Court of International Justice
PKD	Public Key Directory
PMRD	Provincial Market Regulatory Department (China)

QR	Quick Response (machine readable matrix barcode)
QTSP	Qualified Trust Service Provider
RAM	Random Access Memory
RICO	Racketeer Influenced and Corrupt Organizations Act (U.S.)
RKUHP	Draft Code of Criminal Procedure (Indonesia)
RSA	Rivest-Shamir-Adleman (public key crypto system)
SACU	Southern African Customs Union
SADC	Southern African Development Community
SAMR	State Administration for Market Regulation (China)
SAR	Suspicious Activity Report
SATA	SMART Africa Trust Alliance
SDN	Specially Designated Nationals and Blocked Persons (U.S.)
SIM	Subscriber Identity Module (mobile device subscriber identity card)
SRIP	Supervised Remote Identity Proofing
STR	Suspicious Transaction Report
TBML	Trade-Based Money Laundering
TCK	Turkish Penal Code
TCSP	Trust or Company Service Provider
TFEU	Treaty on the Functioning of the European Union
TFR	Transfer of Funds Regulation (EU)
UIF	Unidad de Investigaciones Financieras (Bolivia)
UK	United Kingdom
UN	United Nations
UNCAC	United Nations Convention against Corruption
UNHCR	United Nations High Commissioner for Refugees
UNTOC	United Nations Convention against Transnational Organized Crime
VASP	Virtual Asset Service Provider

References

- Ab Aziz, Norjihan, Noor Shuhadawati Mohamad Amin, and Zuraini Ab Hamid. 2017. Enhancing Plea Bargaining Process through Mediation. *International E-Journal of Advances in Social Sciences (IJASOS)* 3: 306–12. [\[CrossRef\]](#)
- al-Alfi, Ahmad Abd al-Aziz. 1982. Punishment in Islamic Criminal Law. In *The Islamic Criminal Justice System*. Edited by Mahmoud Cherif Bassouni. London: Oceana, pp. 227–36.
- Amicelle, Anthony, and Killian Chaudieu. 2022. The Most Denounced, the Least Punished: Ruling Elites, Illegalisms, and Anti-Money Laundering. *International Political Sociology* 16: olac007. [\[CrossRef\]](#)
- ‘Arafa, Mohamed A. 2018. White-Collar Crimes, Corruption and Bribery in Islamic Criminal Law: Lacuna and Conceivable Paths. *Rule of Law and Anti-Corruption Center Journal* 2018: 3. [\[CrossRef\]](#)
- Attorney General’s Office. 2012. Guidance: The Acceptance of Pleas and the Prosecutor’s Role in the Sentencing Exercise. Available online: <https://www.gov.uk/guidance/the-acceptance-of-pleas-and-the-prosecutors-role-in-the-sentencing-exercise#b-general-principles> (accessed on 22 September 2023).
- AU. 2021. *Report of the 4th Ordinary Session of the STC on Communication and ICT (STC-CICT)*, 25–27 October 2021. Ministerial Session Meeting Report. Addis Ababa: African Union.
- Babaji, Bala, and Ibrahim Danjuma. 2015. The Concept of Plea Bargaining in the Muslims’ Countries: The Islamic Position Towards Its Application. *Journal of Islamic and Comparative Law* 30: 62–73.
- Baker, Donald I. 2001. The Use of Criminal Law Remedies to Deter and Punish Cartels and Bid-Rigging. *George Washington Law Review* 69: 693–714.
- Balogun, Anuoluwapo, Jonathan Aluju, and Wonuola Abioye. 2022. Nigeria. In *Cartels and Leniency 2023*. Edited by Matthew Readings and Elvira Aliende Rodriguez. London: Global Legal Group, pp. 97–102.
- BankID. n.d.a. BankID. Available online: <https://www.bankid.no/en/about-us/> (accessed on 22 September 2023).
- BankID. n.d.b. BankID COI White Paper. Available online: https://confluence-bankidnorge-no.translate.google.com/confluence/kiev-open/bankid-coi-whitepaper/prosess?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp (accessed on 22 September 2023).
- BankID. n.d.c. FAQ. Available online: <https://www.bankid.no/en/private/solve-my-bankid-problem/faq/> (accessed on 22 September 2023).
- Barbosa, Alexandre, Celina Carvalho, Claudio Machado, and Janaina Costa. 2020. *Good ID in Latin America: Strengthening Appropriate Uses of Digital Identity in the Region*. Rio de Janeiro: Instituto de Tecnologia y Sociedade do Rio.
- Bassiouni, Mahmoud Cherif. 1974. Theories of Jurisdiction and Their Application in Extradition Law and Practice. *California Western International Law Journal* 5: 1–61.
- Battini, Stefano. 2011. Globalisation and Extraterritorial Regulation: An Unexceptional Exception. In *Values in Global Administrative Law*. Edited by Gordon Anthony, Jean-Bernard Auby, John Morison and Tom Zwart. New York: Bloomsbury, pp. 61–80.

- Batz, Marie T. 2007. Comparative Analysis of United States and European Union Jurisdiction in Extraterritorial Antitrust Law and the Need for International Standards. *Duquesne Business Law Journal* 9: 65–90.
- Bertrand, Olivier, and Marc Ivaldi. 2006. European Competition Policy in International Markets. *SSRN Electronic Journal*, 1–45. [CrossRef]
- Bicek, Rudolf. 2022. Plea Bargaining: A New Trend in European Criminal Proceedings. Available online: <https://www.schoenherr.eu/content/plea-bargaining-a-new-trend-in-european-criminal-proceedings/> (accessed on 22 September 2023).
- Bilalli-Zendeli, Arta. 2019. Extradition: It's Nature and Scope in Criminal Matters. *JUSTICIA—International Journal of Legal Sciences* 7: 33–43.
- BiometricUpdate.com. 2022. EU Says It Can Have a Digital ID Wallet by '24 Regardless of Challenges. Available online: <https://www.biometricupdate.com/202211/eu-says-it-can-have-a-digital-id-wallet-by-24-regardless-of-challenges> (accessed on 22 September 2023).
- Boister, Neil. 2016. The Cooperation Provisions of the UN Convention against Transnational Organised Crime: A 'Toolbox' Rarely Used? *International Criminal Law Review* 16: 39–70. [CrossRef]
- Bozkurt, Abdullah. 2022. ISIS Commander Granted Leniency at Trial in Turkey and Receives Reduced Sentence. Available online: <https://nordicmonitor.com/2022/01/isis-commander-granted-leniency-in-trial-and-received-a-reduced-sentence-in-turkey/> (accessed on 22 September 2023).
- Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press.
- Brugger, Fritz, Joschka Proksik, and Felicitas Fischer. 2022. The State and the 'Legalization' of Illicit Financial Flows: Trading Gold in Bolivia, WIDER Working Paper 2022/171. WIDER. Available online: <https://www.wider.unu.edu/sites/default/files/Publications/Working-paper/PDF/wp2022-171-state-legalization-illicit-financial-flows-trading-gold-Bolivia.pdf> (accessed on 22 September 2023).
- Burgess, Rachel. 2023. Chapter 26: Association of Southeast Asian Nations. In *Research Handbook on Cartels*. Edited by Peter Whelan. Cheltenham: Edward Elgar, pp. 454–75.
- Burt, Chris. 2019. ID2020 and Partners Launch Program to Provide Digital ID with Vaccines. Available online: <https://www.biometricupdate.com/201909/id2020-and-partners-launch-program-to-provide-digital-id-with-vaccines> (accessed on 22 September 2023).
- Burt, Chris. 2021. ID2020 and Bangladesh Government Issue RFP for Biometrics-Linked Healthcare Digital ID. Available online: <https://www.biometricupdate.com/202104/id2020-and-bangladesh-government-issue-rfp-for-biometrics-linked-healthcare-digital-id> (accessed on 22 September 2023).
- Burt, Chris. 2022. Buenos Aires Planning Ambitious Decentralized Digital Identity System with Biometrics. Available online: <https://www.biometricupdate.com/202205/buenos-aires-planning-ambitious-decentralized-digital-identity-system-with-biometrics> (accessed on 22 September 2023).
- Businesswire. 2023. Over 95% of Indians and Indonesians Hold Digital IDs Linked to Government Databases, Making Document-Free Onboarding a Promising Reality for Businesses. Available online: <https://www.businesswire.com/news/home/20230207005782/en/Over-95-of-Indians-and-Indonesians-hold-digital-IDs-linked-to-government-databases-making-document-free-onboarding-a-promising-reality-for-businesses> (accessed on 22 September 2023).
- Caesar, Ed. 2023. Crooks' Mistaken Bet on Encrypted Phones. Available online: <https://www.newyorker.com/magazine/2023/04/24/crooks-mistaken-bet-on-encrypted-phones> (accessed on 22 September 2023).
- Cammack, Mark E., and R. Michael Feener. 2012. The Islamic Legal System in Indonesia. *Washington International Law Journal* 21: 13–42.
- Carty, James E. 1951. Habeas Corpus in Extradition Proceedings. *Duke Bar Journal* 1: 188–206. [CrossRef]
- Casey, Eoghan. 2002. Practical Approaches to Recovering Encrypted Digital Evidence. *International Journal of Digital Evidence* 1: 1–26.
- Chen, Christopher. 2017. Extraterritoriality of the Regulations and Interconnections of the Derivatives Market: Legal Implications for East and Southeast Asia. *Masaryk University Journal of Law and Technology* 11: 323–49. [CrossRef]
- Chin, Roger J., Gregory Hennessy, and Toby Madubuko. 2015. India's Aadhaar Project: The Unprecedented and Unique Partnership for Inclusion. *Journal of Administrative Science* 12: 1–16.
- CIA. 2023. The World Factbook: Turkey. Available online: <https://www.cia.gov/the-world-factbook/countries/turkey-turkiye/#people-and-society> (accessed on 22 September 2023).
- Clarke, Julie. 2023. Chapter 27: Australia and New Zealand. In *Research Handbook on Cartels*. Edited by Peter Whelan. Cheltenham: Edward Elgar, pp. 476–99.
- Coffee, John C., Jr. 2014. Extraterritorial Financial Regulation: Why E.T. Can't Come Home. *Cornell Law Review* 99: 1259–302.
- CoolBitX. 2020a. Bridge: Enabling VASPs to Collect and Exchange Compliance-Required Transaction Information. Available online: <https://www.sygnia.io/bridge/> (accessed on 17 February 2023).
- CoolBitX. 2020b. *Sygnia Bridge Report: FATF Recommendation 16 Technical Solution for Virtual Asset Transactions*. Arcadia: CoolBitX.
- Corvalan, Camila, and Mariano Plaza. 2022. Argentina. In *Cartels and Leniency 2023*. Edited by Matthew Readings and Elvira Aliende Rodriguez. London: Global Legal Group, pp. 6–11.
- Council of Europe. 2014. *White Paper on Transnational Organised Crime*. Strasbourg: Council of Europe.
- Council of Europe. 2023. Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Available online: <https://www.coe.int/en/web/cybercrime/parties-observers> (accessed on 22 September 2023).

- Cox, Joseph. 2016. 7 Ways the Cops Will Bust You on the Dark Web. Available online: <https://www.vice.com/en/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web> (accessed on 22 September 2023).
- Crijns, Jan H., Marieke J. Dubelaar, and Kelly M. Pitcher. 2017. *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*. Leiden: Leiden University.
- Daijiworld News. 2017. ‘Adhaar’ Most Sophisticated ID Programme in the World: World Bank. Available online: <https://www.daijiworld.com/news/newsDisplay.aspx?newsID=442948> (accessed on 22 September 2023).
- Davis, Nicholas. 2021. The FBI’s Operation Trojan Shield: Infiltrating Criminal Groups through Their Phones. Available online: <https://www.american.edu/sis/centers/security-technology/operation-trojan-shield.cfm#:~:text=The%20FBI%20T1%20textquoterights%20Operation%20Trojan%20Shield%3A%20Infiltrating%20Criminal%20Groups%20through%20their%20Phones,-By%20Nicholas%20Davis&text=On%208%20June%202021%2C%20the,compromised%20phones%20to%20criminal%20groups> (accessed on 22 September 2023).
- de Arruda Sampaio, Onofre Carlos, and Andre Cutait de Arruda Sampaio. 2019. Brazil. In *Cartel Regulation 2020*. Edited by Neil Campbell. London: Law Business Research, pp. 39–46.
- Dictionary.com. 2023. Smartphone. Available online: <https://www.dictionary.com/browse/smart---phone> (accessed on 22 September 2023).
- Digicert. 2022. Secure, Authenticated Signatures with a Single Click. Available online: <https://www.digicert.com/signing/document-signing-certificates> (accessed on 22 September 2022).
- Director of Public Prosecutions South Australia. 2014. *Statement of Prosecution Policy & Guidelines*. Adelaide: Government of South Australia.
- DLA Piper. 2022. *Cartel Enforcement: Global Review—2022*. London: DLA Piper.
- DocuSign. 2022. Understanding Digital Signatures. Available online: <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq#:~:text=A%20digital%20certificate%20is%20an,belongs%20to%20the%20specific%20organization> (accessed on 22 September 2023).
- Egbegi, Tariere. 2020. *The Administration of Criminal Justice Act (ACJA) 2015: Overview and Tools for Protection of the Rights of Women and Children*. Abuja: International Federation of Women Lawyers.
- Emmenegger, Susan. 2016. Extraterritorial Economic Sanctions and Their Foundation in International Law. *Arizona Journal of International and Comparative Law* 33: 631–60.
- ENISA. 2021. *Remote ID Proofing: Analysis of Methods to Carry Out Identity Proofing Remotely*. Athens: ENISA.
- Entrust. 2023. Digital Signing Document Signing Certificates. Available online: <https://www.entrust.com/digital-security/certificate-solutions/products/digital-signing/document-signing-certificates> (accessed on 22 September 2023).
- Estlund, Michelle. 2018. Interpol’s Colorful ‘Notices’ Are Potent, Obscure Tools to Combat Financial Crime. Available online: <https://www.jdsupra.com/legalnews/interpol-s-colorful-notices-are-potent-78535/> (accessed on 22 September 2023).
- European Commission. 2007. Commission Working Document on the Feasibility of EU Legislation in the Area of Protection of Witnesses and Collaborators with Justice /* COM/2007/0693 Final */. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007DC0693&from=SK> (accessed on 22 September 2023).
- European Commission. 2022. European Digital Identity. Available online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (accessed on 22 September 2023).
- Europol. 2020. Sophisticated Case of Money Laundering Leads to 15 Arrests in Malta. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/sophisticated-case-of-money-laundering-leads-to-15-arrests-in-malta> (accessed on 22 September 2023).
- Ezrachi, Ariel, and Jiri Kindl. 2011. Cartels as Criminal? The Long Road from Unilateral Enforcement to International Consensus. In *Criminalising Cartels: Critical Studies of an International Regulatory Movement*. Edited by Caron Beaton-Wells and Ariel Ezrachi. Bloomsbury: Bloomsbury, pp. 419–34.
- FATF. 2014. *Transparency and Beneficial Ownership*. Paris: FATF.
- FATF. 2018. *Professional Money Laundering*. Paris: FATF.
- FATF. 2019a. *FATF 30 Years—1989–2019*. Paris: FATF.
- FATF. 2019b. *Virtual Assets and Virtual Asset Service Providers*. Paris: Financial Action Task Force.
- FATF. 2021. Who We Are. Available online: <https://www.fatf-gafi.org/en/the-fatf/who-we-are.html> (accessed on 22 September 2023).
- FATF. 2023. *Guidance on Beneficial Ownership for Legal Persons*. Paris: FATF.
- FBI. 2021. FBI’s Ability to Legally Access Secure Messaging App Content and Metadata. Available online: <https://propertyofthepeople.org/document-detail/?doc-id=21114562> (accessed on 22 September 2023).
- FBI. n.d. Ross William Ulbricht’s Laptop. Available online: <https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop> (accessed on 22 September 2023).
- FEDPOL. 2014. Jugements Prononcés en Suisse en Matière de Blanchiment d’Argent. Available online: <https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/jb.html> (accessed on 22 September 2023).
- FinCEN. 2014. Report of Cash Payments over \$10,000 Received in a Trade or Business. Available online: <https://www.irs.gov/pub/irs-s-pdf/f8300.pdf> (accessed on 22 September 2023).
- FinCEN. 2016. Customer Due Diligence Requirements for Financial Institutions, Appendix A. Available online: <https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf> (accessed on 22 September 2023).

- Franceschi-Bicchierai, Lorenzo. 2022. This Is the 'Graykey 2.0,' the Tool Cops Use to Hack Phones. Available online: <https://www.vice.com/en/article/93an8a/this-is-the-graykey-20-the-tool-cops-use-to-hack-phones> (accessed on 22 September 2023).
- Freeman, Michelle A., and David A. Hickerson. 2023. Prepare for Extraterritorial Enforcement of U.S. Antitrust Law. Available online: <https://www.foley.com/en/insights/publications/2023/03/prepare-extraterritorial-enforcement-us-antitrust> (accessed on 22 September 2023).
- Fukami, Aya, Radina Stoykova, and Zeno Geradts. 2021. A New Model for Forensic Data Extraction from Encrypted Mobile Devices. *Forensic Science International: Digital Investigation* 38: 301169. [CrossRef]
- Fyfe, Nicholas, and James Sheptycki. 2005. *Facilitating Witness Co-Operation in Organised Crime Cases: An International Review*. Online Report No. 27/05. London: UK Home Office.
- Fyfe, Nicholas, and James Sheptycki. 2006. International Trends in the Facilitation of Witness Co-Operation in Organized Crime Cases. *European Journal of Criminology* 3: 319–55. [CrossRef]
- Gallant, Kenneth S. 2022. *International Criminal Jurisdiction: Whose Law Must We Obey?* Oxford: Oxford University Press.
- Garrote, Marina, Nathan Paschoalini, and Marina Meira. n.d. Why Should We All Pay Attention to the Brazilian Digital ID System? Available online: <https://www.dataprivacybr.org/en/documentos/why-should-we-all-pay-attention-to-the-brazilian-digital-id-system/> (accessed on 22 September 2023).
- Gibson Dunn. 2020. *Developments in the Defense of Financial Institutions: The International Reach of the U.S. Money Laundering Statutes*. Los Angeles: Gibson Dunn.
- GlobalSign. 2023. Gmo Globalsign Unveils New Solution for Secure, Trusted High-Volume Seals. Available online: <https://www.globalsign.com/en/company/news-events/news/gmo-globalsign-unveils-new-solution-secure-trusted-high-volume-seals> (accessed on 22 September 2023).
- GSMA. 2022. *The State of Mobile Internet Connectivity 2022*. London: GSMA.
- Guliani, Priya. 2022. Identity for Social and Financial Inclusion. In *Impact of Women's Empowerment on SDGs in the Digital Era*. Edited by Ingrid Vasiliu-Feltes. Hershey: IGI Global, pp. 79–99.
- Gutiérrez, Juan David. 2023. Chapter 28: South America. In *Research Handbook on Cartels*. Edited by Peter Whelan. Cheltenham: Edward Elgar, pp. 500–20.
- Hadjiyianni, Ioanna. 2021. The European Union as a Global Regulatory Power. *Oxford Journal of Legal Studies* 41: 243–64. [CrossRef]
- Hersey, Frank. 2023. World Bank Proposes \$250m for Indonesia Digital ID for Public and Private Service Access. Available online: <https://www.biometricupdate.com/202301/world-bank-proposes-250m-for-indonesia-digital-id-for-public-and-private-service-access> (accessed on 22 September 2023).
- Hodgson, Jacqueline. 2012. Guilty Pleas and the Changing Role of the Prosecutor in French Criminal Justice. In *The Prosecutor in Transnational Perspective*. Edited by Erik Luna and Marianne Wade. Oxford: Oxford University Press, pp. 116–34.
- Hodgson, Jacqueline, and Laurene Soubise. 2016. Understanding the Sentencing Process in France. *Crime and Justice: Review of Research* 45: 221–66. [CrossRef]
- Hodgson, Jacqueline S. 2020. *The Metamorphosis of Criminal Justice: A Comparative Account*. New York: Oxford University Press.
- Hughes, Graham. 1992. Agreements for Cooperation in Criminal Cases. *Vanderbilt Law Review* 45: 1–70.
- IBM. 2023. Digital Certificates for User Authentication. Available online: <https://www.ibm.com/docs/en/i/7.3?topic=dcu-digital-certificates-user-authentication> (accessed on 22 September 2023).
- ICAO. 2023a. Access to ePassport Chip. Available online: <https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Document-reader.aspx> (accessed on 22 September 2023).
- ICAO. 2023b. ePassport Validation. Available online: <https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Validation.aspx> (accessed on 22 September 2023).
- ICIJ. 2020. Global Banks Defy U.S. Crackdowns by Serving Oligarchs, Criminals and Terrorists: The FinCEN Files Show Trillions in Tainted Dollars Flow Freely through Major Banks, Swamping a Broken Enforcement System. Available online: <https://www.icij.org/investigations/fincen-files/global-banks-defy-u-s-crackdowns-by-serving-oligarchs-criminals-and-terrorists/> (accessed on 22 September 2023).
- ID2020. 2016. ID2020 Holds Inaugural Summit at the United Nations. Available online: <https://medium.com/id2020/id2020-holds-inaugural-summit-at-the-united-nations-7112014add5e#:~:text=In%20May%202016%2C%20at%20the,any%20form%20of%20recognized%20identification.> (accessed on 22 September 2023).
- IdenTrust. 2023. Apply Trusted Digital Signatures to Your Documents. Available online: <https://www.identrust.com/digital-certificates/document-signing> (accessed on 22 September 2023).
- InterFax. 2023. Putin Backs Digital Development Ministry's Proposal to Introduce Digital IDs on Smartphones. Available online: <https://interfax.com/newsroom/top-stories/88011/> (accessed on 22 September 2023).
- INTERPOL. 2023. Member Countries. Available online: <https://www.interpol.int/en/Who-we-are/Member-countries#:~:text=INTERPOL%20has%20195%20member%20countries,police%20with%20our%20global%20network> (accessed on 22 September 2023).
- IOSCO. 2023. Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU). Available online: <https://www.iosco.org/about/?subsection=mmou> (accessed on 22 September 2023).
- Iqbal, Saman. 2022. Criminal Justice Reform—Revamping Pakistan's Colonial Structures. Available online: <https://rsilpak.org/2022/criminal-justice-reform-revamping-pakistans-colonial-structures/> (accessed on 22 September 2023).

- Ireland-Piper, Danielle. 2012. Extraterritorial Criminal Jurisdiction: Does the Long Arm of the Law Undermine the Rule of Law. *Melbourne Journal of International Law* 13: 122–57.
- Ismail, Halima Umami. 2021. Plea Bargaining and the Islamic Criminal Justice System. Available online: <https://loyalnigerianlawyer.com/plea-bargaining-and-the-islamic-criminal-justice-system/> (accessed on 22 September 2023).
- Iwasokun, Gabriel Babatunde, Taiwo Gabriel Omomule, and Raphael Olufemi Akinyede. 2018. Encryption and Tokenization-Based System for Credit Card Information Security. *International Journal of Cyber-Security and Digital Forensics* 7: 283–93. [CrossRef]
- Jamieson, Alison. 2000. *The Antimafia: Italy's Fight against Organized Crime*. New York: St. Martin's Press.
- Janis, Mark W. 2003. *An Introduction to International Law*, 4th ed. New York: Aspen.
- Joelson, Mark R. 2017. The Application of United States Antitrust Law to International Transactions and Foreign Parties. In *An International Antitrust Primer: A Guide to the Operation of United States, European Union and Other Key Competition Laws in the Global Economy*. Edited by Mark R. Joelson. Zuid-Holland: Kluwer Law International, pp. 43–66.
- Jones Day. 2012. Cartel Leniency in the Asia-Pacific Region. Available online: <https://www.jonesday.com/en/insights/2012/05/carte-leniency-in-the-asia-pacific-region> (accessed on 22 September 2023).
- Joshua, Julian M., Peter D. Camesasca, and Youngjin Jung. 2008. Extradition and Mutual Legal Assistance Treaties: Cartel Enforcement's Global Reach. *Antitrust Law Journal* 75: 353–98.
- Jung, Youngjin. 2005. Korean Competition Law: First Step Towards Globalization. *Journal of Korean Law* 4: 177–99.
- Kageyama, Yuri. 2022. Japan Steps up Push to Get Public Buy-In to Digital IDs. Available online: <https://apnews.com/article/technology-health-japan-covid-public-d47817295a647379f69da9bb16160d13> (accessed on 22 September 2023).
- Kaira, Thula. 2017. Cartel Enforcement in the Southern African Neighborhood. In *Competition Law and Economic Regulation: Addressing Market Power in Southern Africa*. Edited by Jonathan Klaaren, Simon Roberts and Imraan Valodia. Johannesburg: Wits University Press, pp. 71–96.
- Kianersi, Nima, Mohsen Shekarchizadeh, and Masoud Zamani. 2022. Plea Bargaining in the Criminal Law of the US and Iran and Its Effect on Diversion with a Jurisprudential Approach. *Economic Jurisprudence Studies* 3: 105–20.
- Kiunuhe, Anne, and Njeri Wagacha. 2019. Kenya. In *Cartel Regulation 2020*. Edited by Neil Campbell. London: Law Business Research, pp. 152–61.
- Knott, Ryan Paul. 2010. Extraterritoriality, the Effects Doctrine and Enforcement Cooperation through Bilateral Agreements with Regards to Antitrust Law. L.L.M. thesis, University of Johannesburg, Johannesburg, South Africa.
- Kolasky, William. 2004. Criminalising Cartel Activity: Lessons from the U.S. Experience. *Competition and Consumer Law Journal* 12: 207–23.
- Krotoski, Mark. 2015. "Extradition in International Antitrust Enforcement Cases". The Antitrust Source. Available online: <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/antitrust-source-extradition-in-international-antitrust-enforcement-cases-april2015.pdf?rev=dc351fa5d406459899e9f1ef3ed596ce&hash=6EA478111B109163A51061F5F4A35533> (accessed on 22 October 2023).
- Kursun, Eren, Gene Fernandez, Alex Berson, and Brian Goodman. 2018. *System and Method for Biometric Authentication-Based Electronic Notary Public*. Alexandria: USPTO.
- Kyprianou, Despina. 2006. The Role of the Cyprus Attorney General's Office in Prosecutions: Rhetoric, Ideology and Practice. Ph.D. thesis, University of London, London, UK.
- Langer, Máximo. 2021. Plea Bargaining, Conviction without Trial, and the Global Administratization of Criminal Convictions. *Annual Review of Criminology* 4: 377–411. [CrossRef]
- Lee, Belinda S., Meaghan P. Thomas-Kennedy, and Elizabeth C. Gettinger. 2022. Korea. In *Cartels: Enforcement, Appeals and Damages Actions 2022*. Edited by Euan Burrows and Denis Fosselard. London: Global Legal Group, pp. 192–201.
- Lessambo, Felix I. 2020. Extraterritorial Competence of the United States, the EU, and China Competition Laws. In *Mergers in the Global Markets: A Comparative Approach to the Competition and National Security Laws among the US, EU, and China*. Edited by Felix I. Lessambo. Cham: Springer International Publishing, pp. 133–65.
- Liang, Ding. 2019. China. In *Cartel Regulation 2020*. Edited by Neil Campbell. London: Law Business Research, pp. 59–67.
- Library of Congress. 2013. Brazil: New Law Defines "Criminal Organization" and Provides for Investigatory and Other Procedures. Available online: [https://www.loc.gov/item/global-legal-monitor/2013-08-12/brazil-new-law-defines-criminal-organization-and-provides-for-investigatory-and-other-procedures/#:~:text=12.850%2C%20de%20%20de%20Agosto,such%20organizati%20\(art%201\)](https://www.loc.gov/item/global-legal-monitor/2013-08-12/brazil-new-law-defines-criminal-organization-and-provides-for-investigatory-and-other-procedures/#:~:text=12.850%2C%20de%20%20de%20Agosto,such%20organizati%20(art%201)) (accessed on 22 September 2023).
- Liu, Bo Ning. 2020. Observation of Judicial Promise in the System of "Leniency in Confession and Punishment Acceptance". *Legal Science* 2020: 50–64.
- Macdonald, Ayang. 2022a. China to Introduce Digital ID Cards Nationwide. Available online: <https://www.biometricupdate.com/202203/china-to-introduce-digital-id-cards-nationwide> (accessed on 22 September 2023).
- Macdonald, Ayang. 2022b. Norway to Replace BankID on Mobile with Biometric Apps for Improved Security. Available online: <https://www.biometricupdate.com/202205/norway-to-replace-bankid-on-mobile-with-biometric-apps-for-improved-security> (accessed on 22 September 2023).
- Mackarel, Mark, and Susan Nash. 1997. Extradition and the European Union. *International and Comparative Law Quarterly* 46: 948–57.
- Mahlangu, Philile Lomthandazo. 2014. Enforcement against Cartels in South African Competition Law: Advantages and Challenges. Master's thesis, University of Pretoria, Pretoria, South Africa.

- Majozi, Nkosinathi Levion. 2019. Plea Bargaining in South Africa and England. L.L.M. thesis, University of Pretoria, Pretoria, South Africa.
- Malik, Hasnaat. 2021. Govt Plans to Insert Chapter of Plea Bargain in CrPC. Available online: <https://tribune.com.pk/story/2322720/govt-plans-to-insert-chapter-of-plea-bargain-in-crpc> (accessed on 22 September 2023).
- Mark, Gideon. 2018. The Yates Memorandum and Cartel Enforcement. *UC Davis Law Review Online* 51: 95–119.
- Mascellino, Alessandro. 2022. Japan to Integrate Health Insurance Cards into My Number Digital ID in Digitization Push. Available online: <https://www.biometricupdate.com/202210/japan-to-integrate-health-insurance-cards-into-my-number-digital-id-in-digitization-push> (accessed on 22 September 2023).
- Mathew, Basil B. 2014. Aadhaar Project: A Critical Analysis. *International Interdisciplinary Research Journal* 4: 476–83.
- Meheretu, Alemu. 2016. The Proposed Plea Bargaining in Ethiopia: How It Fares with Fundamental Principles of Criminal Law and Procedure. *Mizan Law Review* 10: 400–29. [CrossRef]
- Melendez, Steven. 2019. How to Open a MoneyGram Account. Available online: <https://www.sapling.com/12030173/open-moneygram-account> (accessed on 22 September 2023).
- Ministry of Justice. 2003. *Federal Democratic Republic of Ethiopia Criminal Justice Policy*. Addis Ababa: Ministry of Justice.
- Ministry of Justice. 2019. Présentation Des Dispositions Immédiatement Applicables de La Loi N°2019-222 Du 23 Mars 2019 de Programmation 2018–2022 Et de Réforme Pour La Justice Relatives Aux Alternatives Aux Poursuites, Aux Poursuites Et Au Jugement [Presentation of the Immediately Applicable Provisions of Law No. 2019-222 of March 23, 2019 of 2018–2022 Programming and Reform for Justice Relating to Alternatives to Prosecution, Prosecution and Judgment]. Available online: <http://www.justice.gouv.fr/bo/2019/20190430/JUSD1910286C.pdf> (accessed on 22 September 2023).
- MONEYVAL. 2015. *Typologies Report on Laundering the Proceeds of Organised Crime*. Strasbourg: Council of Europe.
- MOSIP. n.d.a. An Open Source Platform on Which National Foundational IDs Are Built. Available online: <https://www.mosip.io/ind-ex.php> (accessed on 22 September 2023).
- MOSIP. n.d.b. What Is MOSIP? Available online: <https://www.mosip.io/about.php> (accessed on 22 September 2023).
- Murray, Kenneth. 2016. In the Shadow of the Dark Twin: Proving Criminality in Money Laundering Cases. *Journal of Money Laundering Control* 19: 447–58. [CrossRef]
- Muzata, Tapera, Simon Roberts, and Thando Vilakazi. 2017. Penalties and Settlements for South African Cartels: An Economic Review. In *Competition Law and Economic Regulation: Addressing Market Power in Southern Africa*. Edited by Jonathan Klaaren, Simon Roberts and Imraan Valodia. Johannesburg: Wits University Press, pp. 13–48.
- Nadelmann, Ethan A. 1990. The Role of the United States in the International Enforcement of Criminal Law. *Harvard International Law Journal* 31: 37–76.
- Nagashima Ohno & Tsunematsu. 2020. Court Rules in Japan’s First Plea Bargaining Case. Available online: <https://www.lexology.com/commentary/white-collar-crime/japan/nagashima-ohno-tsunematsu/court-rules-in-japans-first-plea-bargaining-case#Plea%20bargaining%20system> (accessed on 22 September 2023).
- NCA. 2020. NCA and Police Smash Thousands of Criminal Conspiracies after Infiltration of Encrypted Communication Platform in UK’s Biggest Ever Law Enforcement Operation. Available online: <https://nationalcrimeagency.gov.uk/news/operation-venetic?highlight=WyjlbmNyb2NoYXQiLCJlbmNyb2NoYXQncyJd> (accessed on 22 September 2023).
- Negash, Alemu Meheretu. 2018. Rethinking Plea Bargaining Policy: The Case of Ethiopia. *Mizan Law Review* 11: 342–72. [CrossRef]
- Nikel, David. 2022. BankID: Norway’s Digital ID System Explained. Available online: <https://www.lifeinnorway.net/bankid-norway/> (accessed on 22 September 2023).
- Nishioka, Kazuaki. 2020. International Scope of the Japanese Anti-Monopoly Act in Cross-Border Cartel Cases: A Japanese Approach to ‘Extraterritorial Application’. *Journal of Antitrust Enforcement* 8: 590–605. [CrossRef]
- NIST. n.d.a. Biometrics Collection. Available online: <https://pages.nist.gov/800-63-3-Implementation-Resources/63A/biometrics/> (accessed on 22 September 2023).
- NIST. n.d.b. Supervised Remote Identity Proofing. Available online: <https://pages.nist.gov/800-63-3-Implementation-Resources/63A/srip/> (accessed on 22 September 2023).
- Oddie, Carolyn, and Felicity McMahon. 2022. Australia. In *Cartel Regulation 2023*. Edited by Andrew Neil Campbell. London: Law Business Research, pp. 6–15.
- OECD. 2016. *Exchange of Information on Request: Handbook for Peer Reviews 2016–2020: 2016 Terms of Reference*. Paris: OECD.
- OECD. 2018. *Standard for Automatic Exchange of Financial Account Information in Tax Matters*, 2nd ed. Paris: OECD.
- OECD. 2021. *Building Effective Beneficial Ownership Frameworks: A Joint Global Forum and IDB Toolkit*. Paris: OECD.
- OECD. 2022. *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. Paris: OECD.
- OECD. 2023. Automatic Exchange of Information (AEOI): Status of Commitments. Available online: <https://www.oecd.org/tax/transparency/AEOI-commitments.pdf> (accessed on 22 September 2023).
- OECD. n.d.a. Global Forum on Transparency and Exchange of Information for Tax Purposes: Issuing Ratings. Available online: <https://www.oecd.org/tax/transparency/what-we-do/> (accessed on 22 September 2023).
- OECD. n.d.b. Exchange of Information on Request: A Robust and Transparent Review Process. Available online: <https://www.oecd.org/tax/transparency/documents/exchange-of-information-on-request-peer-review-process.htm> (accessed on 22 September 2023).

- Ohlson, Mark, Anthony Lo, and Fran Wang. 2013. Taiwan. In *Cartel Regulation in 46 Jurisdictions Worldwide 2014*. Edited by Andrew Neil Campbell. London: Law Business Research, pp. 305–11.
- Owens, Jeffrey P., and Rick McDonell. 2018. *Creating Mechanisms to Get Good Access to Beneficial Ownership Information in International Context*. Vienna: Vienna University of Economics and Business.
- Oxenham, John, and Maria Webber. 2013. South Africa. In *Cartel Regulation in 46 Jurisdictions Worldwide 2014*. Edited by Andrew Neil Campbell. London: Law Business Research, pp. 272–79.
- Parnell Law Chambers. 2021. Interpol Red Notice and the International Extradition Law. Available online: <https://www.parnellchambers.co.nz/index.php/practice-areas/interpol-red-notice-and-the-international-extradition-law/> (accessed on 22 September 2023).
- Pascu, Luana. 2020. Argentina Enables Remote Digital ID Processing for Mobile During COVID-19 Crisis. Available online: <https://www.biometricupdate.com/202004/argentina-enables-remote-digital-id-processing-for-mobile-during-covid-19-crisis> (accessed on 22 September 2023).
- Pathak, Apurva. 2015. Plea Bargaining: A New Chapter in Indian Legal System. *International Journal of Research in Humanities & Social Sciences* 3: 53–56.
- Peters and Peters. n.d. The London Scheme on Extradition within the Commonwealth. Available online: [https://extraditionuk.petersandpeters.com/extradition/resources/the-london-scheme-on-extradition-within-the-commonwealth/#:~:text=The%20London%20Scheme%20on%20Extradition%20within%20the%20Commonwealth%20\(%E2%80%9Cthe%20London,Scheme%20was%20amended%20in%202000](https://extraditionuk.petersandpeters.com/extradition/resources/the-london-scheme-on-extradition-within-the-commonwealth/#:~:text=The%20London%20Scheme%20on%20Extradition%20within%20the%20Commonwealth%20(%E2%80%9Cthe%20London,Scheme%20was%20amended%20in%202000) (accessed on 22 September 2023).
- Pfefferkorn, Riana. 2021. We Now Know What Information the FBI Can Obtain from Encrypted Messaging Apps. Available online: <https://www.justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/> (accessed on 22 September 2023).
- Plachta, Michael. 1999. *Aut Dedere Aut Judicare: An Overview of Modes of Implementation and Approaches*. *Maastricht Journal of European and Comparative Law* 6: 331. [CrossRef]
- Prete, Luca. 2018. On Implementation and Effects: The Recent Case-Law on the Territorial (or Extraterritorial?) Application of EU Competition Rules. *Journal of European Competition Law & Practice* 9: 487–95. [CrossRef]
- PYMNTS. 2022. OneSpan, BankID Extend Digital Identity Service to All Norwegian Banks. Available online: <https://www.pymnts.com/digital-identity/2022/onespan-bankid-extend-digital-identity-service-all-norwegian-banks/> (accessed on 22 September 2023).
- Raza, Muhammad Subtain, Qi Zhan, and Sana Rubab. 2020. Role of Money Mules in Money Laundering and Financial Crimes: A Discussion through Case Studies. *Journal of Financial Crime* 27: 911–31. [CrossRef]
- ReadID. 2023. Which Countries Have ePassports? Available online: <https://www.readid.com/blog/countries-epassports> (accessed on 22 September 2023).
- Reims, Raphael. 2022. The Criminal Prosecution of Hardcore Cartels in the USA and the EU—A Backdoor Criminalization in the EU by the USA? *Competition Policy International* 2022: 1–9.
- Republic of Ethiopia. 2013. *Criminal Law Procedure and Law of Evidence (Draft)*. Addis Ababa: Republic of Ethiopia.
- Reuters. 2021. Italy Judge Convicts 70 People in Major Mafia Trial. Available online: <https://www.reuters.com/world/italy-judge-convicts-70-people-major-mafia-trial-2021-11-08/> (accessed on 22 September 2023).
- Said, Mark. 2022. The Plea-Bargain Conundrum. Available online: <https://www.independent.com.mt/articles/2022-04-14/newspaper-opinions/The-plea-bargain-conundrum-6736242197> (accessed on 22 September 2023).
- Sathe, Vijay. 2011. The World's Most Ambitious ID Project. *Innovations in Education and Teaching International* 6: 39–66.
- Schloenhardt, Andreas. 2021. International Cooperation under the United Nations Convention against Transnational Organized Crime: Expectations and Experiences. *Brill Research Perspectives in Transnational Crime* 3: 3–25. [CrossRef]
- Schwartz, Jeffrey. 2016. Fighting for a Secure Digital Identity for All. Available online: <https://redmondmag.com/Articles/2016/07/01/Common-Cause.aspx?Page=2&m=1> (accessed on 22 September 2023).
- Scott, Joanne. 2014. The New EU 'Extraterritoriality'. *Common Market Law Review* 51: 1343–80. [CrossRef]
- Scotti, Benjamin. 2002. Rico vs. 416-bis: A Comparison of US and Italian Anti-Organized Crime Legislation. *Loyola of Los Angeles International and Comparative Law Review* 25: 143–64.
- Seddon, Judith, Eleanor Davison, Christopher J. Morvillo, Michael Bowes QC, Luke Tolaini, Ama A. Adams, and Tara McGrath, eds. 2021. *The Practitioner's Guide to Global Investigations, Vol. 1: Global Investigations in the United Kingdom and the United States*, 6th ed. London: Global Investigations Review.
- Seethal, Dana S., and Roger Ramgoolam. 2019. *Commonwealth Caribbean Criminal Practice and Procedure*, 5th ed. London: Routledge.
- Sentencing Council. 2023. Sentencing Guidelines for Use in Crown Court. Available online: <https://www.sentencingcouncil.org.uk/offences/crown-court/item/fraud/> (accessed on 22 September 2023).
- Shaffer, Gregory C., Nathaniel H. Nesbitt, and Spencer W. Waller. 2015. Criminalizing Cartels: A Global Trend? In *Comparative Competition Law*. Edited by John Duns, Arlen Duke and Brendan Sweeney. Cheltenham: Edward Elgar, pp. 301–44.
- Sharma, Vikas. 2011. Aadhaar—A Unique Identification Number: Opportunities and Challenges Ahead. *Research Cell: An International Journal of Engineering Sciences* 4: 169–78.
- Shi, Jiahui. 2021. Reconsideration of the Role of Prosecutors in the Chinese Plea Bargaining System: A Comparative Perspective. *Chinese Studies* 10: 88–99. [CrossRef]

- Shirk, David A. 2016. Criminal Justice Reform in Mexico: An Overview. *Mexican Law Review* 3: 189–228.
- Sigler, Heather J. 2009. Federal Criminal Conspiracy. *American Criminal Law Review* 46: 589–620.
- SMART Africa Alliance. 2020a. *SMART Africa Alliance: Digital Identity: Blueprint*. Kigali: SMART Africa Alliance.
- SMART Africa Alliance. 2020b. Who We Are. Available online: <https://smartafrica.org/who-we-are/> (accessed on 22 September 2023).
- Smart Card Alliance. 2009. *ePassport Frequently Asked Questions*. Princeton Junction: Smart Card Alliance.
- Sogut, Koray. 2019. Significant Amendments to the Code of Criminal Procedure Under the First Package of the Judicial Reform. Available online: <https://www.esin.av.tr/2019/10/30/significant-amendments-to-the-code-of-criminal-procedure-under-the-first-package-of-the-judicial-reform/> (accessed on 22 September 2023).
- Solomon, Peter H., Jr. 2012. Plea Bargaining Russian Style. *Demokratizatsiya: The Journal of Post-Soviet Democratization* 20: 282–99.
- SS8 Networks. n.d. *The Ready Guide to Intercept Legislation*. San Jose: SS8 Networks.
- Sumsb. n.d. *Streamlining Identity Verification in Emerging Markets*. London: Sumsb.
- Tak, Peter J. P. 1997. Deals with Criminals: Supergrasses, Crown Witnesses and Pentiti. *European Journal of Crime, Criminal Law and Criminal Justice* 5: 2–26. [CrossRef]
- TASS. 2019. Russia to Roll out Digital IDs in 2024. Available online: <https://tass.com/science/1044074> (accessed on 22 September 2023).
- Thales. 2023. Biometrics: Definition, Use Cases, Latest News. Available online: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics> (accessed on 22 September 2023).
- Theodorou, Yiannis. 2022. On the Road to Digital-ID Success in Africa: Leveraging Global Trends. Available online: <https://institute.global/policy/road-digital-id-success-africa-leveraging-global-trends#:~:text=A%20recent%20report%20for%20that,to%20present%20online%20and%20offline> (accessed on 22 September 2023).
- Thomas, Christopher, and Gianni De Stefano. 2016. “Extradition and Antitrust: Cautionary Tales for Global Cartel Compliance”. AB Extra. Available online: https://www.hoganlovells.com/~/_media/hogan-lovells/pdf/publication/hogan_lovell_ab_extra_30_09_16.pdf (accessed on 22 October 2023).
- Tinsley, Alex. 2021. Specialty: Arresting an Elusive ‘Right’ in European Extradition Law. *New Journal of European Criminal Law* 12: 23–35. [CrossRef]
- Tristanto, Yunizar Wahu. 2018. Juridical Review of Implementation of Plea Bargaining for Improving Justice Efficiency in Indonesia. *AHKAM* 6: 411–36.
- Tuan, Nguyen Anh, Tran Hai Thinh, and Tran Hoang My. 2019. Vietnam. In *Cartel Regulation 2020*. Edited by Neil Campbell. London: Law Business Research, pp. 298–305.
- U.S. Department of Justice. 2020a. 18 U.S.C. § 371—Conspiracy to Defraud the United States. Available online: <https://www.justice.gov/v/archives/jm/criminal-resource-manual-923-18-usc-371-conspiracy-defraud-us> (accessed on 22 September 2023).
- U.S. Department of Justice. 2020b. 2161. Jury Instruction: Intent to Promote the Carrying on of the Specified Unlawful Activity. Available online: <https://www.justice.gov/archives/jm/criminal-resource-manual-2161-jury-instruction-intent-promote-carrying-specified-unlawful#:~:text=The%20term%20with%20the%20intent,of%20the%20crimes%20listed%20as> (accessed on 22 September 2023).
- U.S. Department of Justice. 2020c. 2166. Jury Instruction: Conspiracy to Commit Money Laundering. Available online: <https://www.justice.gov/archives/jm/criminal-resource-manual-2166-jury-instruction-conspiracy-commit-money-laundering> (accessed on 22 September 2023).
- U.S. Department of the Treasury. 2023. Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists. Available online: <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx> (accessed on 22 September 2023).
- U.S. Mission Panama. 2022. Panama Intermediaries Each Sentenced to 36 Months in Prison for International Bribery and Money Laundering. Available online: <https://pa.usembassy.gov/panama-intermediaries-each-sentenced-to-36-months-in-prison-for-international-bribery-and-money-laundering-scheme/> (accessed on 22 September 2023).
- UN. 2023. Vienna Convention on the Law of Treaties: Status. Available online: https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXIII-1&chapter=23&Temp=mtdsg3&clang=_en (accessed on 22 September 2023).
- UNHCR. 2018. Announcing the 2018 ID2020 Summit—Towards “Good” Digital Identity. Available online: <https://www.unhcr.org/bl ogs/announcing-the-2018-id2020-summit-towards-good-digital-identity/> (accessed on 22 September 2023).
- United Nations. 2023. United Nations Convention against Transnational Organized Crime: Status. Available online: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en (accessed on 22 September 2023).
- University of Oxford. 2023. Our World in Data. Available online: <https://ourworldindata.org/grapher/median-daily-per-capita-expenditure-vs-gdp-per-capita?tab=table> (accessed on 22 September 2023).
- UNODC. 2006. *Legislative Guide for the Implementation of the United Nations Convention against Corruption*. U.N. Sales No. E.06.IV.16. Vienna: UNODC.
- UNODC. 2019. Extradition. Available online: <https://www.unodc.org/e4j/zh/organized-crime/module-11/key-issues/extradition.html> (accessed on 22 September 2023).
- UNODC. 2021. *Digest of Cases of International Cooperation in Criminal Matters Involving the United Nations Convention against Transnational Organized Crime as a Legal Basis*. Vienna: UNODC.

- USDOJ. 2020. Two Alleged Criminals—A Hezbollah Associated Narco-Money Launderer and a Computer Hacker—Extradited from Cyprus to the United States. Available online: <https://www.justice.gov/opa/pr/two-alleged-criminals-hezbollah-associated-narco-money-launderer-and-computer-hacker> (accessed on 22 September 2023).
- van der Does de Willebois, Emile, Emily M. Halter, Robert A. Harrison, Park Ji Won, and Jason C. Sharman. 2011. *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*. Washington, DC: The International Bank for Reconstruction and Development.
- van der Wilt, Harmen. 2022. *The Law and Practice of Extradition*. Abingdon: Routledge.
- Ventura, Manuel J. 2019. Aiding and Abetting. In *Modes of Liability in International Criminal Law*. Edited by Jérôme de Hemptinne, Robert Roth, Elies van Sliedregt, Marjolein Cupido, Manuel J. Ventura and Lachezar Yanev. Cambridge: Cambridge University Press, pp. 173–256.
- Wagner, Benjamin B., and Leslie Gielow Jacobs. 2008. Retooling Law Enforcement to Investigate and Prosecute Entrenched Corruption: Key Criminal Procedure Reforms for Indonesia and Other Nations. *University of Pennsylvania Journal of International Law* 30: 183–265.
- Warin, F. Joseph. 2013. The Global Reach of American Criminal Law. Available online: <https://www.gibsondunn.com/wp-content/uploads/documents/publications/Warin-TheGlobalReachofAmericanCriminalLaw-0213.pdf> (accessed on 22 September 2023).
- Watanabe, Eriko, and Koki Yanagisawa. 2019. Japan. In *Cartel Regulation 2020*. Edited by Neil Campbell. London: Law Business Research, pp. 143–51.
- Wells Fargo. 2021. Certification Regarding Beneficial Owners of Legal Entity Customers. Available online: <https://www08.wellsfargo.com/assets/pdf/small-business/beneficial-owner.pdf> (accessed on 22 September 2023).
- West, David. 2019. Extradition. In *Commonwealth Caribbean Criminal Practice and Procedure*. Edited by Roger Ramgoolam. London: Routledge, pp. 394–412.
- Won-cheol, Kim. 2006. Extraterritorial Application of Antitrust Law to International Cartels. *Corporate Law Research* 20: 385–409.
- World Bank. 2017. *The State of Identification Systems in Africa*. Washington: World Bank.
- Wydra, Elizabeth B. 2004. Is an Overt Act an Element of the Crime of Conspiracy to Commit Money Laundering (03-1293) (03-1294). *Preview of United States Supreme Court Cases 2004*: 146–50.
- Yeh, Stuart S. 2020a. An International Law Approach to End Money Laundering. *Journal of International Banking Law and Regulation* 35: 148–63.
- Yeh, Stuart S. 2020b. An International Treaty to Fight Money Laundering. *Journal of International Banking Law and Regulation* 35: 190–207.
- Yeh, Stuart S. 2020c. Application of a Model International Treaty to Money Laundering. *Journal of International Banking Law and Regulation* 35: 443–62.
- Yeh, Stuart S. 2021. APUNCAC: An International Convention to Fight Corruption, Money Laundering, and Terrorist Financing. *Law and Development Review* 14: 633–64. [\[CrossRef\]](#)
- Yeh, Stuart S. 2022a. New Financial Action Task Force Recommendations to Fight Corruption and Money Laundering. *Laws* 11: 8. [\[CrossRef\]](#)
- Yeh, Stuart S. 2022b. *The End of Corruption and Impunity*. New York: Lexington.
- Yoon, Hoil, Sinsung Yun, and Kenneth T. Kim. 2016. Korea. In *Cartel Regulation*. Edited by Andrew Neil Campbell. London: Law Business Research, pp. 136–43.
- Zabrodin, Vladislav, and Irina Akimova. 2012. Cartel Regulation—2013: The Application of Competition Regulation in 48 Jurisdictions Worldwide—Russia. Available online: <https://www.cls.ru/press-centr/publications/cartel-regulation---2013/> (accessed on 22 September 2023).
- Zanotti, Isidoro. 2006. *Extradition in Multilateral Treaties and Conventions*. Vol. 3, Studies on the Law of Treaties. Leiden: Martinus Nijhoff.
- Zerk, Jennifer A. 2010. *Extraterritorial Jurisdiction: Lessons for the Business and Human Rights Sphere from Six Regulatory Areas*. Cambridge: Harvard University.
- Zhou, Qiang. 2017. *Middle-Term Report of the Supreme Court and Supreme People's Procuratorate on the Experiment of Plea Bargaining in Certain Regions*. Beijing: People's Court Post.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.